IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

WEBROOT, INC. and OPEN TEXT, INC.,	§	
	§	
Plaintiffs	§	
	§	
v.	§	NO. 6:22-cv-239-ADA-DTG
	§	
TREND MICRO INC.,	§	JURY TRIAL DEMANDED
	§	
Defendant.	§	
	§	
	§	
TREND MICRO INC.,	§	
	§	
Counter-Plaintiff	§	
	§	
v.	§	
	§	
WEBROOT, INC. and OPEN TEXT, INC.,	§	
	§	
Counter-Defendants,	§	
	§	
and	§	
	§	
OPEN TEXT CORP.	§	
Counter-Defendant.	§	

TRENDMICRO INC.'S ANSWER, AFFIRMATIVE DEFENSES, AND COUNTERCLAIMS TO PLAINTIFFS WEBROOT, INC. AND OPEN TEXT, INC.'S COMPLAINT FOR PATENT INFRINGEMENT

Defendant Trend Micro Inc. ("Trend Micro"), by and through the undersigned attorneys hereby respond to the Complaint for Patent Infringement ("Complaint") filed March 4, 2022 by Plaintiffs Webroot, Inc. ("Webroot") and Open Text, Inc. ("Open Text, Inc."), (collectively, "Plaintiffs"). Trend Micro denies all allegations set forth in the Complaint unless expressly admitted in the following paragraphs. In so doing, Trend Micro denies any allegations contained in Plaintiffs' headings.

Trend Micro's specific responses to the numbered allegations of the Complaint are in the below numbered paragraphs as follows:

1. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 1, and therefore denies them.

2. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 2, and therefore denies them.

3. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 3, and therefore denies them.

4. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 4, and therefore denies them.

5. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 5, and therefore denies them.

6. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 6, and therefore denies them.

7. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 7, and therefore denies them.

8. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 8, and therefore denies them.

9. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 9, and therefore denies them.

10. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 10, and therefore denies them.

11. Trend Micro lacks knowledge or information sufficient to form a belief as to the

truth of the allegations of Paragraph 11, and therefore denies them.

12. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 12, and therefore denies them.

13. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 13, and therefore denies them.

14. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 14, and therefore denies them.

15. Trend Micro admits that it provides Apex One, Smart Protection Network, Deep Security, and Cloud One Workload Security. Trend Micro denies committing any acts of infringement and denies that its products implement Plaintiffs' patented technologies. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 15.

16. Denied.

NATURE OF THE CASE

17. To the extent that the allegations of Paragraph 17 set forth legal conclusions, no response is required. Trend Micro admits the Complaint purports to set forth a patent infringement action arising under the patent laws of the United States. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 17.

THE PARTIES

18. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 18, and therefore denies them.

19. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 19, and therefore denies them.

20. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 20, and therefore denies them.

21. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 21, and therefore denies them.

22. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 22, and therefore denies them.

23. Trend Micro admits that it has a principal place of business at 225 East John Carpenter Freeway Suite 1500, Irving, Texas 75062. Trend Micro admits that it maintains an office at 11305 Alterra Parkway, Austin, Texas 78758. Trend Micro further admits that it is registered with the Secretary of State to conduct business in Texas. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 23.

JURISDICTION & VENUE

24. To the extent that the allegations of Paragraph 24 set forth legal conclusions, no response is required. Trend Micro admits the Complaint purports to set forth a patent infringement action arising under the patent laws of the United States. Trend Micro admits that this Court has subject matter jurisdiction over actions arising under the patent laws of the United States pursuant to 28 U.S.C. §§ 1331 and 1338(a).

25. Trend Micro admits it has transacted business in the state of Texas and in this District. Trend Micro, for purposes of this case only, will not challenge personal jurisdiction in this Court. Trend Micro denies committing any acts of infringement. The remaining allegations of Paragraph 25 regard jurisdiction, which is an issue of law for which no response is required. To the extent a response is required, Trend Micro is without knowledge or information sufficient to form a belief as to the truth of the remaining allegations in Paragraph 25. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 25.

26. Trend Micro admits that it sells, directly or through its distribution network,

products with the knowledge that those products will be sold and/or used nationwide, including in the Western District of Texas. Trend Micro denies committing any acts of infringement. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 26.

27. To the extent that the allegations of Paragraph 27 set forth legal conclusions, no response is required. Trend Micro denies committing any acts of infringement. Trend Micro admits that it did not dispute that this district is a proper forum for venue in the case Plaintiffs cite, but only for purpose of that case. *See, e.g.*, Answer ¶ 9, *Invicta Networks, Inc. v. Trend Micro Inc.*, No. 6:20-cv-00766-ADA, Dkt. 9 (W.D. Tex. Nov. 16, 2020) ("Defendant does not contest that venue is proper under 28 U.S.C. §§ 1391 and 1400(b) ***solely for the purposes of this action***, but denies that venue in this District is convenient or in the interests of justice."). Trend Micro does not dispute venue solely for purposes of this litigation. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 27.

28. To the extent that the allegations of Paragraph 28 set forth legal conclusions, no response is required. Defendant does not contest that it is subject to personal jurisdiction in this District, solely for purposes of this action. Defendant admits that it conducts business in this judicial district ("District"), but denies having committed any acts constituting patent infringement and/or inducing and/or contributing to patent infringement in this District or any District. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 28.

29. To the extent that the allegations of Paragraph 29 set forth legal conclusions, no response is required. Defendant does not contest that it is subject to personal jurisdiction in this District, solely for purposes of this action. Defendant admits that it conducts business in this District, but denies having committed any acts constituting patent infringement and/or inducing

and/or contributing to patent infringement in this District or any District. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 29.

30. To the extent that the allegations of Paragraph 30 set forth legal conclusions, no response is required. Defendant does not contest that it is subject to personal jurisdiction in this District, solely for purposes of this action. Defendant admits that it conducts business in this District, but denies having committed any acts constituting patent infringement and/or inducing and/or contributing to patent infringement in this District or any District. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 30.

31. To the extent that the allegations of Paragraph 31 set forth legal conclusions, no response is required. Defendant does not contest that it is subject to personal jurisdiction in this District, solely for purposes of this action. Defendant admits that it conducts business in this District, but denies having committed any acts constituting patent infringement and/or inducing and/or contributing to patent infringement in this District or any District. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 31.

32. Denied.

33. Denied.

34. Denied.

35. Denied.

36. Denied.

37. Denied.

38. Denied.

PLAINTIFFS' PATENTED INNOVATIONS

39. Trend Micro lacks knowledge or information sufficient to form a belief as to the

truth of the allegations of Paragraph 39, and therefore denies them.

40. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 39, and therefore denies them.

Advanced Malware Detection Patents
U.S. Patent Nos. 8,418,250 and 8,726,389

41. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 41, and therefore denies them.

42. Trend Micro admits what purports to be a copy of the ’250 Patent is attached as Exhibit 1. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 42.

43. Trend Micro admits what purports to be a copy of the ’389 Patent is attached as Exhibit 2. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 43.

44. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 44, and therefore denies them.

45. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 45, and therefore denies them.

46. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 46, and therefore denies them.

47. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 47, and therefore denies them.

48. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 48, and therefore denies them.

49. Trend Micro lacks knowledge or information sufficient to form a belief as to the

truth of the allegations of Paragraph 49, and therefore denies them.

50. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 50, and therefore denies them.

51. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 51, and therefore denies them.

52. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 52, and therefore denies them.

53. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 53, and therefore denies them.

54. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 54, and therefore denies them.

55. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 55, and therefore denies them.

56. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 56, and therefore denies them.

57. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 57, and therefore denies them.

58. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 58, and therefore denies them.

59. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 59, and therefore denies them.

60. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 60, and therefore denies them.

61. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 61, and therefore denies them.

62. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 62, and therefore denies them.

Forensic Visibility Patents
U.S. Patent No. 9,578,045 and U.S. Patent No. 10,257,224

63. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 63, and therefore denies them.

64. Trend Micro admits what purports to be a copy of the ’045 Patent is attached as Exhibit 3. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 42.

65. Trend Micro admits what purports to be a copy of the ’224 Patent is attached as Exhibit 4. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 42.

66. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 66, and therefore denies them.

67. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 67, and therefore denies them.

68. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 68, and therefore denies them.

69. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 69, and therefore denies them.

70. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 70, and therefore denies them.

71. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 71, and therefore denies them.

72. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 72, and therefore denies them.

73. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 73, and therefore denies them.

74. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 74, and therefore denies them.

75. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 75, and therefore denies them.

76. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 76, and therefore denies them.

U.S. Patent No. 10,284,591

77. Trend Micro admits what purports to be a copy of the ’591 Patent is attached as Exhibit 5. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 42.

78. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 78, and therefore denies them.

79. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 79, and therefore denies them.

80. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 80, and therefore denies them.

81. Trend Micro lacks knowledge or information sufficient to form a belief as to the

truth of the allegations of Paragraph 81, and therefore denies them.

U.S. Patent No. 10, 599,844

82. Trend Micro denies that a true and correct copy of the ’844 Patent is attached to the Complaint as Exhibit 6. Exhibit 6 of the Complaint purports to be U.S. Patent No. 10,499,844, not U.S. Patent No. 10,599,844. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations of Paragraph 82, and therefore denies them.

83. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 83, and therefore denies them.

84. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 84, and therefore denies them.

85. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 85, and therefore denies them.

86. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 86, and therefore denies them.

87. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 87, and therefore denies them.

88. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 88, and therefore denies them.

89. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 89, and therefore denies them.

90. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 90, and therefore denies them.

ACCUSED PRODUCTS

91. Denied.

92. Trend Micro admits that it provides Apex One, Apex Central, Cloud One Network Security, and Deep Discovery. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 92.

93. Denied.

94. Denied.

95. Denied.

96. Denied.

97. Denied.

98. Denied.

99. Denied.

FIRST CAUSE OF ACTION
(INFRINGEMENT OF THE ’250 PATENT)

100. Trend Micro incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

101. Denied.

102. Trend Micro admits what purports to be claim 1 of the ’250 Patent is recited in Paragraph 102 of the Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 102.

103. Trend Micro admits that Paragraph 103 purports to include an image from a document available on the webpage at https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?utm_campaign=BaU2021_Endpoint-Security_AoM&utm_medium=Search&utm_source=Google&utm_content=Apex-One-Case, which

states that "A range or layered detection capabilities, alongside investigation and response, defends the endpoint through every stage." Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 103.

104. Trend Micro admits that the document available at https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_ag.pdf states at page 9-22: "Security Agents log unauthorized program access instances and send the logs to the server." Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 104.

105. Denied.

106. Trend Micro admits that Paragraph 106 purports to include an image from a document available on the webpage at https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3a-icon-datasheet-e4288a. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 106.

107. Denied.

108. Denied.

109. Denied.

110. Trend Micro admits that Paragraph 110 purports to include an image from a document available on the webpage at https://www.trendmicro.com/en_us/business/capabilities/machine-learning.html, which states that "Trend Micro whitelisting technology works with machine learning to pro-actively identify good files to reduce false positives." Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 110.

111. Denied.

112. Denied.

113. Trend Micro admits that the document available at

https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_ag.pdf states at page 4-5: "By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides 'better together' security, much like an automated neighborhood watch that involves the community in the protection of others." Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 113.

114. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 114, and therefore denies them.

115. Trend Micro admits that it became aware of the '250 Patent after receiving Plaintiffs' Complaint. Trend Micro denies that it had knowledge of the '250 Patent at any time before receiving Plaintiffs' Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 115.

116. Denied.

117. Denied.

118. Denied.

119. Denied.

120. Denied.

121. Denied.

122. Denied.

123. Denied.

124. Denied.

125. Denied.

126. Denied.

127. Trend Micro admits that it became aware of the ’250 Patent after receiving Plaintiffs’ Complaint. Trend Micro denies that it had knowledge of the ’250 Patent at any time before receiving Plaintiffs’ Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 127.

128. Denied.

SECOND CAUSE OF ACTION
(INFRINGEMENT OF THE ’389 PATENT)

129. Trend Micro incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

130. Denied.

131. Trend Micro admits what purports to be claim 1 of the ’389 Patent is recited in Paragraph 131 of the Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 131.

132. Trend Micro admits that the document available at https://help.deepsecurity.trendmicro.com/12_0/on-premise/Deep_Security_12.0_On-Premise_Administration_Guide.pdf states at page 777: “To identify threats, the anti-malware module checks files on the local hard drive against a comprehensive threat database. The anti-malware module also checks files for certain characteristics, such as compression and known exploit code.” Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 132.

133. Denied.

134. Trend Micro admits that Paragraph 134 purports to include an image from a document available on the webpage at https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3a-icon-datasheet-e4288a. Except as expressly admitted,

Trend Micro denies the remaining allegations of Paragraph 134.

135. Denied.

136. Trend Micro admits that Paragraph 136 purports to include images from a webpage at https://success.trendmicro.com/dcx/s/solution/000262137?language=en_US. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 136.

137. Trend Micro admits that the document available at https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_ag.pdf states at page 4-3: "Smart Protection includes services that provide anti-malware signatures, web reputations, and threat databases that are stored in-the-cloud." Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 137.

138. Trend Micro admits that the document available at https://help.deepsecurity.trendmicro.com/12_0/on-premise/Deep_Security_12.0_On-Premise_Administration_Guide.pdf states at page 997: "The log inspection feature in Deep Security enables real-time analysis of third party log files. The log inspection rules and decoders provide a framework to parse, analyze, rank and correlate events across a wide variety of systems. As with intrusion prevention and integrity monitoring, log inspection content is delivered in the form of rules included in a security update." Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 138.

139. Denied.

140. Trend Micro admits that the document available at https://help.deepsecurity.trendmicro.com/12_0/on-premise/Deep_Security_12.0_On-Premise_Administration_Guide.pdf states at page 814: "Deep Security Manager will be able to retrieve the suspected object list from Trend Micro Apex Central, share it with protected computers, and compare local objects against the Apex Central Suspicious Object List." Except

as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 140.

141. Trend Micro admits that the document available at https://help.deepsecurity.trendmicro.com/12_0/on-premise/Deep_Security_12.0_On-Premise_Administration_Guide.pdf states at page 814: "Deep Security Manager will be able to retrieve the suspected object list from Trend Micro Apex Central, share it with protected computers, and compare local objects against the Apex Central Suspicious Object List." Trend Micro further admits that the document states at page 777: "To identify threats, the anti-malware module checks files on the local hard drive against a comprehensive threat database. The anti-malware module also checks files for certain characteristics, such as compression and known exploit code." Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 141.

142. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 142, and therefore denies them.

143. Trend Micro admits that became aware of the '389 Patent after receiving Plaintiffs' Complaint. Trend Micro denies that it had knowledge of the '389 Patent at any time before receiving Plaintiffs' Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 143.

144. Denied.

145. Denied.

146. Denied.

147. Denied.

148. Denied.

149. Denied.

150. Denied.

151. Denied.

152. Denied.

153. Denied.

154. Denied.

155. Trend Micro admits that became aware of the ’389 Patent after receiving Plaintiffs’ Complaint. Trend Micro denies that it had knowledge of the ’389 Patent at any time before receiving Plaintiffs’ Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 155.

156. Denied.

THIRD CAUSE OF ACTION
(INFRINGEMENT OF THE ’045 PATENT)

157. Trend Micro incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

158. Denied.

159. Trend Micro admits what purports to be claim 1 of the ’045 Patent is recited in Paragraph 159 of the Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 159.

160. Denied.

161. Denied.

162. Denied.

163. Denied.

164. Denied.

165. Denied.

166. Denied.

167. Denied.

168. Trend Micro admits that Paragraph 168 purports to include an image from a webpage at https://www.trendmicro.com/en_in/what-is/xdr.html. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 168.

169. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 169, and therefore denies them.

170. Trend Micro admits that became aware of the ’045 Patent after receiving Plaintiffs’ Complaint. Trend Micro denies that it had knowledge of the ’045 Patent at any time before receiving Plaintiffs’ Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 170.

171. Denied.

172. Denied.

173. Denied.

174. Denied.

175. Denied.

176. Denied.

177. Denied.

178. Denied.

179. Denied.

180. Denied.

181. Denied.

182. Trend Micro admits that it became aware of the ’045 Patent after receiving Plaintiffs’ Complaint. Trend Micro denies that it had knowledge of the ’045 Patent at any time

before receiving Plaintiffs' Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 182.

183. Denied.

FOURTH CAUSE OF ACTION
(INFRINGEMENT OF THE '244 PATENT)

184. Trend Micro incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

185. Denied.

186. Trend Micro admits what purports to be claim 1 of the '244 Patent is recited in Paragraph 186 of the Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 186.

187. Denied.

188. Denied.

189. Denied.

190. Denied.

191. Denied.

192. Denied.

193. Trend Micro admits that Paragraph 193 purports to include an image from a webpage at https://www.trendmicro.com/en_in/what-is/xdr.html. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 193.

194. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 194, and therefore denies them.

195. Trend Micro admits that it became aware of the '244 Patent after receiving Plaintiffs' Complaint. Trend Micro denies that it had knowledge of the '244 Patent at any time

before receiving Plaintiffs' Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 195.

196. Denied.

197. Denied.

198. Denied.

199. Denied.

200. Denied.

201. Denied.

202. Denied.

203. Denied.

204. Denied.

205. Denied.

206. Denied.

207. Trend Micro admits that became aware of the '244 Patent after receiving Plaintiffs' Complaint. Trend Micro denies that it had knowledge of the '244 Patent at any time before receiving Plaintiffs' Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 207.

208. Denied.

FIFTH CAUSE OF ACTION
(INFRINGEMENT OF THE '591 PATENT)

209. Trend Micro incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

210. Denied.

211. Trend Micro admits what purports to be claim 1 of the '591 Patent is recited in

Paragraph 211 of the Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 211.

212. Denied.

213. Denied.

214. Trend Micro admits that Paragraph 212 purports to include an image from a webpage at https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 214.

215. Trend Micro admits that the webpage available at https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats states: "The Microsoft framework is also capable of accessing application programming interfaces (APIs) that execute crucial system and application functions." Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 215.

216. Denied.

217. Trend Micro admits that the document available at https://docs.trendmicro.com/all/ent/apex-one/2019/en-us/apexOne_2019_ag.pdf states at page 1-2: "Security Agent policies provide increased real-time protection against the latest fileless attack methods through enhanced memory scanning for suspicious process behaviors. Security Agents can terminate suspicious processes before any damage can be done." Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 217.

218. Denied.

219. Denied.

220. Trend Micro admits that the webpage available at https://help.deepsecurity.trendmicro.com/20_0/on-premise/anti-malware-behavior-monitoring.html

states: “Structured Exception Handling Overwrite Protection (SEHOP), and heap spray prevention, Deep Security can determine whether a process has been compromised and then terminate the process to prevent further infection.” Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 220.

221. Denied.

222. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 222 and therefore denies them.

223. Trend Micro admits that it became aware of the ’591 Patent after receiving Plaintiffs’ Complaint. Trend Micro denies that it had knowledge of the ’591 Patent at any time before receiving Plaintiffs’ Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 223.

224. Denied.

225. Denied.

226. Denied.

227. Denied.

228. Denied.

229. Denied.

230. Denied.

231. Denied.

232. Denied.

233. Denied.

234. Denied.

235. Trend Micro admits that it became aware of the ’591 Patent after receiving

Plaintiffs' Complaint. Trend Micro denies that it had knowledge of the '591 Patent at any time before receiving Plaintiffs' Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 235.

236. Denied.

SIXTH CAUSE OF ACTION
(INFRINGEMENT OF THE '844 PATENT)

237. Trend Micro incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

238. Denied.

239. Trend Micro admits what purports to be claim 1 of the '844 Patent is recited in Paragraph 239 of the Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 239.

240. Denied.

241. Trend Micro admits that the webpage available at https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/predictive-machine-l.aspx states: "After detecting an unknown or low-prevalence file, the Security Agent scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features and sends the report to the Predictive Machine Learning engine, hosted on the Trend Micro Smart Protection Network." Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 241.

242. Denied.

243. Trend Micro admits that Paragraph 243 purports to include an image from a webpage at https://www.trendmicro.com/vinfo/mx/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-

behavioral-features. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 243.

244. Denied.

245. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 245 and therefore denies them.

246. Denied.

247. Denied.

248. Denied.

249. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 249 and therefore denies them.

250. Trend Micro lacks knowledge or information sufficient to form a belief as to the truth of the allegations of Paragraph 250 and therefore denies them.

251. Trend Micro admits that it became aware of the ’844 Patent after receiving Plaintiffs’ Complaint. Trend Micro denies that it had knowledge of the ’844 Patent at any time before receiving Plaintiffs’ Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 251.

252. Denied.

253. Denied.

254. Denied.

255. Denied.

256. Denied.

257. Denied.

258. Denied.

259. Denied.

260. Denied.

261. Denied.

262. Denied.

263. Trend Micro admits that it became aware of the ’844 Patent after receiving Plaintiffs’ Complaint. Trend Micro denies that it had knowledge of the ’844 Patent at any time before receiving Plaintiffs’ Complaint. Except as expressly admitted, Trend Micro denies the remaining allegations of Paragraph 263.

264. Denied.

RESPONSE TO PLAINTIFFS’ PRAYER FOR RELIEF

To the extent a response is required, Trend Micro denies that Plaintiffs are entitled to any relief sought in its Prayer for Relief and denies that Plaintiffs are entitled to any relief whatsoever.

RESPONSE TO PLAINTIFFS’ JURY DEMAND

To the extent a response is required Trend Micro admits that the Complaint contains a request for a jury trial.

AFFIRMATIVE DEFENSES

Without admitting or acknowledging that Trend Micro bears the burden of proof as to any of them and reserving the right to amend its answer as additional information becomes available, Trend Micro pleads the following defenses:

FIRST DEFENSE
(Non-Infringement)

Trend Micro has not engaged in any acts that would constitute willful, direct or indirect infringement of any valid claim of any of the ’250 Patent, the ’389 Patent, the ’045 Patent, the ’224 Patent, the ’591 Patent, or the ’844 Patent (collectively, the “Patents-in-Suit”) either literally or under the doctrine of equivalents.

SECOND DEFENSE
(Invalidity)

The Patents-in-Suit are invalid because they do not satisfy the requirements of 35 U.S.C. § 100, *et seq.*, including but not limited to, 35 U.S.C. §§ 101, 102, 103, 112 and/or 116.

THIRD DEFENSE
(Prosecution History Estoppel / Prosecution Disclaimer)

Plaintiffs’ claims are barred in whole or in part by the doctrines of prosecution history estoppel and/or prosecution disclaimer.

FOURTH DEFENSE
(Ensnarement)

Plaintiffs’ claims are barred or limited by the doctrine of ensnarement.

FIFTH DEFENSE
(Limitation on Damages)

Plaintiffs’ right to seek damages, if any, is limited by 35 U.S.C. §§ 286, 287, and 288.

SIXTH DEFENSE
(Territoriality)

To the extent Plaintiffs’ claims are directed to acts occurring outside the United States, those claims for relief are barred or limited by the doctrine of territoriality by 35 U.S.C. § 271 et seq. including but not limited to § 271(a) and (c).

SEVENTH DEFENSE
(Failure to State a Claim)

Plaintiffs have failed to state a claim upon which relief can be granted.

EIGHTH DEFENSE
(Double Patenting)

One or more of the asserted claims is invalid under the doctrine of statutory double patenting or the judicially–created doctrine of obviousness-type double patenting.

NINTH DEFENSE
(Lack of Standing)

To the extent Plaintiffs lacks all substantive right to bring suit and to exclude others from practicing the claims of one or more the Patents-in-Suit, Plaintiffs' claims are barred by a lack of standing.

TENTH DEFENSE
(Judicial Estoppel)

Plaintiffs' patent infringement claims are barred, in whole or in part, based on judicial estoppel. The asserted claims of the Patents-in-Suit are invalid or unenforceable, and Trend Micro has not infringed, and is not infringing, the asserted claims of the Patents-in-Suit at least due in part to statements, representation, admissions, elections, positions, concessions, and filings made by Plaintiffs in prior judicial or administrative proceedings.

ELEVENTH DEFENSE
(Res Judicata and/or Collateral Estoppel)

Plaintiffs' claims, and issues relating to those claims, are barred, in whole or in part, as a result of adjudications on the merits of other judicial or administrative proceedings involving the Patents-in-Suit.

TWELFTH DEFENSE
(Waiver, Unclean Hands, orEquitable Estoppel)

Plaintiffs' claims are barred, in whole or in part, under the doctrines of waiver, unclean hands, and/or equitable estoppel.

THIRTEENTH DEFENSE
(License and/or Patent Exhaustion)

Plaintiffs' patent infringement claims are barred, in whole or in part, under the doctrines of express license, implied license, and/or patent exhaustion.

FOURTEENTH DEFENSE
(Government Sales)

Plaintiffs' remedies are limited by 28 U.S.C. § 1498(a).

FIFTEENTH DEFENSE
(Misjoinder of Parties)

Plaintiffs are misjoined in this action to the extent that they are seeking to enforce rights that exist independent of one another and have no apparent link to one another, or to the extent any of them lack standing to bring this suit.

RESERVATION OF DEFENSES

Trend Micro reserves all affirmative defenses under Rule 8(c) of the Federal Rules of Civil Procedure, the Patent Laws of the United States, and any other defenses, at law or in equity, that may now exist or in the future be available based on discovery and future factual investigation.

DEMAND FOR JURY TRIAL

Trend Micro demands a jury trial on all triable issues.

TREND MICRO'S COUNTERCLAIMS

1. Pursuant to Rule 13 of the Federal Rules of Civil Procedure, Trend Micro counterclaims against Counter-Defendants Open Text, Inc. and Open Text Corporation ("Open Text Corp.") (hereinafter collectively as "Open Text"), and Webroot, Inc. ("Webroot"), Open Text Corp. being joined pursuant to Rule 20(a)(2) of the Federal Rules of Civil Procedure, asserting the following Counterclaims.

NATURE OF THE ACTION

2. Trend Micro is a leading cyber security software company that protects businesses and individuals against various cyber threats. Trend Micro operates a portfolio of products and services that allow people to use their computers, mobile phones, tablets, and various other electronic devices to safely and securely. Trend Micro invented many innovative products, including those that are cloud-based and utilize machine learning and artificial intelligence technologies. Some of these innovative inventions include those covered by U.S. Patent Nos. 8,838,992 and 8,051,487 (collectively, the "Trend Micro Patents-in-Suit").

3. Trend Micro seeks to enjoin infringement and obtain damages resulting from Counter-Defendants Webroot's and Open Text's unauthorized making, using, offering for sale, and/or selling software and/or services, including related software and services, that implement the patented technologies in the Trend Micro Patents-in-Suit.

PARTIES

4. Trend Micro Inc. is a corporation organized and existing under the laws of the State of California, with its principal place of business at 225 East John Carpenter Freeway, Suite 1500 Irving, Texas 75062. Among other activities, it is in the business of providing cyber security software to protect individuals and businesses against malware, spam, and other cyber

threats. Trend Micro has customers throughout the United States, the State of Texas, and in this district.

5. Webroot is a corporation organized and existing under the laws of Delaware, with its principal place of business at 385 Interlocken Crescent Suite 800 Broomfield, CO 80021. Webroot practices and provides, contributes to practicing and providing, and induces others to practice and provide methods and systems that infringe claims of each of Trend Micro's Patents-in-Suit.

6. Open Text, Inc. is a corporation organized and existing under the laws of Delaware, with its principal place of business at Suites 301&302, 2440 Sand Hill Road, Menlo Park, CA 94025. Open Text, Inc. practices and provides, contributes to practicing and providing, and induces others to practice and provide methods and systems that infringe claims of each of Trend Micro's Patents-in-Suit.

7. Open Text Corp. is a corporation organized and existing under the laws of Ontario, Canada, with its principal place of business at 275 Frank Tompa Dr. Waterloo ON, N2L 0A1. Open Text Corp. practices and provides, contributes to practicing and providing, and induces others to practice and provide methods and systems that infringe claims of each of Trend Micro's Patents-in-Suit.

JURISDICTION AND VENUE

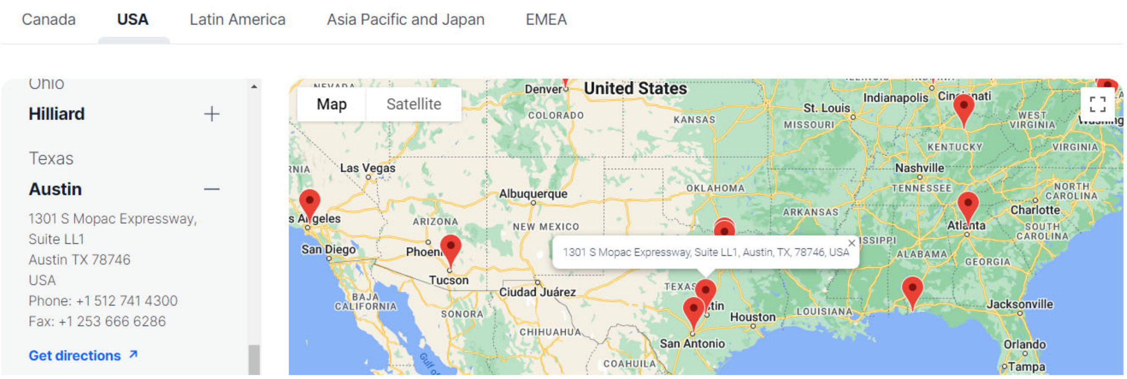
8. Counter-Plaintiff Trend Micro's counterclaim arises under Title 35 of the United States Code. This Court has subject matter jurisdiction over Trend Micro's patent infringement claims pursuant to 28 U.S.C §§ 1331 and 1338.

9. This Court has personal jurisdiction over Open Text Inc. and Webroot, *inter alia*, based on filing of the Complaint.

10. This Court has personal jurisdiction over Open Text Corp., *inter alia*, because it regularly conducts business in the State of Texas and in this District, including operating systems, using software, providing services, and/or engaging in activities in Texas and in this District that infringe one or more claims of the asserted Patents.

11. Counter-Defendant Open Text Corp. has, either directly and through its network of partnerships, purposefully and voluntarily placed its infringing products and/or provided services into the stream of commerce with the intention and expectation that they will be purchased and used by customers in this District, as detailed below.

12. Open Text Corp. maintains three offices in the State of Texas, two of which are located in this judicial district, including the Austin office and the San Antonio office. *See Open Text Corp. v. Alfresco Software, Ltd.*, No. 6:20-cv-00941, Dkt. No. 1 (Complaint) ¶ 9; *see also* https://www.opentext.com/about/office-locations#austin-address.



Canada USA Latin America Asia Pacific and Japan EMEA

Ohio

Hilliard +

Texas

Austin —

1301 S Mopac Expressway,
Suite LL1
Austin TX 78746
USA
Phone: +1 512 741 4300
Fax: +1 253 666 6286

Get directions ↗

1301 S Mopac Expressway, Suite LL1, Austin, TX, 78746, USA

13. Open Text Corp.'s Austin office includes employees in engineering, customer support legal and compliance teams, IT, and corporate development, and it hosts one of Open Text Corp.'s data centers. *See Open Text Corp. v. Alfresco Software, Ltd.*, No. 6:20-cv-00941, Dkt. No. 1 (Complaint) ¶ 9.

14. Open Text Corp.'s partners, including resellers, distributors, service providers, support partners, and technology partners are located in this judicial district. *See*

https://www.opentext.com/products-and-solutions/partners-and-alliances/partner-directory.

15. In addition, OpenText Professional Services Agreement states that the agreement is entered into by Open Text Corp. or one of its affiliates and its customers. *See* https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-psa-pdf.pdf. Thus, Open Text Corp. has entered into agreements with customers covering infringing products and/or provided services in Texas and in this District.

16. Venue is proper in this District as to these Counterclaims against Webroot and Open Text, Inc. pursuant to 28 U.S.C §§ 1391(a)-(c) and 1400(b) because, *inter alia*, Webroot and Open Text, Inc. have submitted to the venue of this Court by filing its Complaint here.

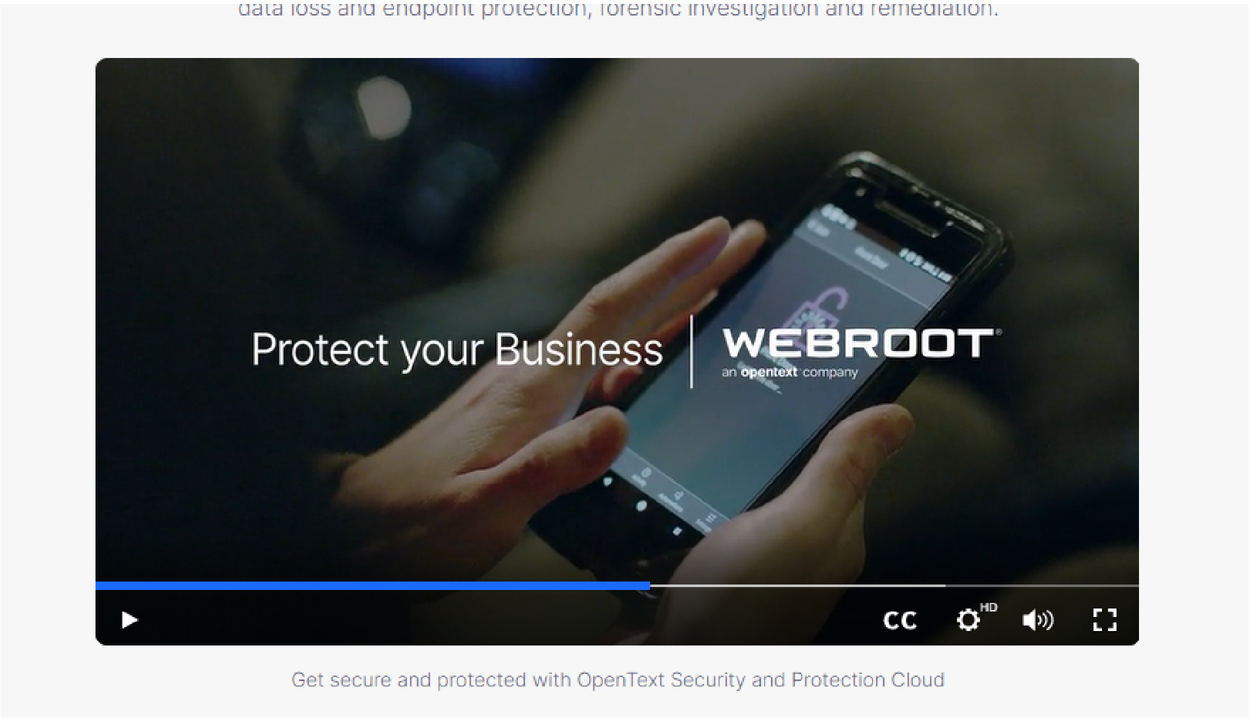
17. Venue is proper in this District as to these Counterclaims against Open Text Corp. pursuant to 28 U.S.C. §§ 1391(b) and (c) and 28 U.S.C. § 1400(b) because Open Text Corp. is a foreign corporation and may be sued in any district in the United States, including this District.

ACCUSED PRODUCTS

18. Webroot offers security software, systems, and services that implement Trend Micro's patented technologies, such as, but not limited to, Webroot SecureAnywhere Business Endpoint Protection, Webroot SecureAnywhere Endpoint Protection, Webroot DNS Protection, Webroot Wifi Security, and BrightCloud Threat Intelligence Services ("Webroot Accused Products").

19. Open Text offers information management software, systems, and services that implement Trend Micro's patented technologies, such as, but not limited to, OpenText Enterprise & Content Management, OpenText Business Network, OpenText AI & Analytics, OpenText Experience, OpenText Digital Process Automation, OpenText Discovery, and

OpenText Security ("Open Text Accused Products"). *See Open Text Corp. v. Alfresco Software, Ltd.*, No. 6:20-cv-00941 (WDTX), Dkt. No. 1 (Complaint) ¶¶ 5-6; *UnoWeb Virtual, LLC v. Open Text Inc.*, No. 2:19-cv-8 (EDTX), Dkt. No. 19 (Answer) ¶ 13. As one example, Open Text packages Webroot's security services with its information management products, such as with OpenText Security & Protection Cloud that lists Webroot as a product which it integrates with. The following screenshot is taken from a marketing video on the OpenText Security & Protection Cloud product webpage on Open Text's website, found at https://www.opentext.com/products-and-solutions/products/opentext-cloud/opentext-security-cloud, and shows that Webroot's software, systems, and services are part of OpenText's Security & Protection Cloud.

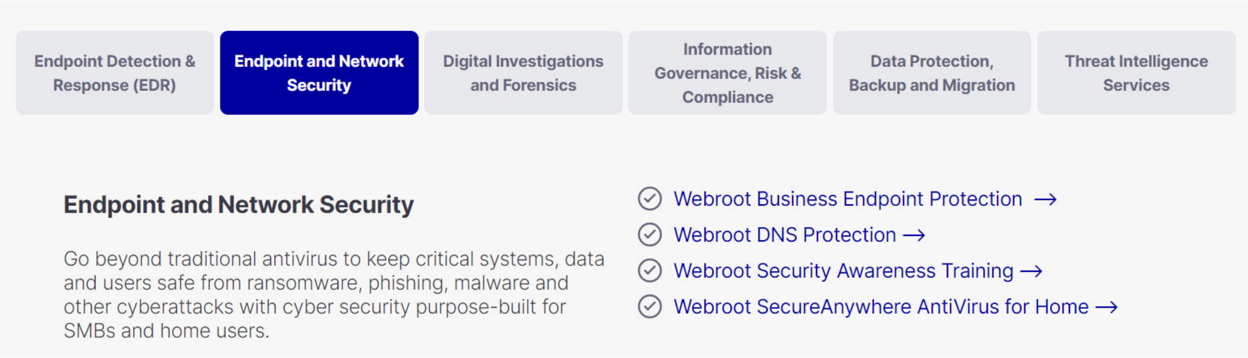


data loss and endpoint protection, forensic investigation and remediation.

Get secure and protected with OpenText Security and Protection Cloud

20. The following screenshot is also taken from the same webpage (https://www.opentext.com/products-and-solutions/products/opentext-cloud/opentext-security-

cloud). This screenshot further shows that the Endpoint and Network Security of the OpenText Security & Protection Cloud comprises Webroot's security software, systems, and services.

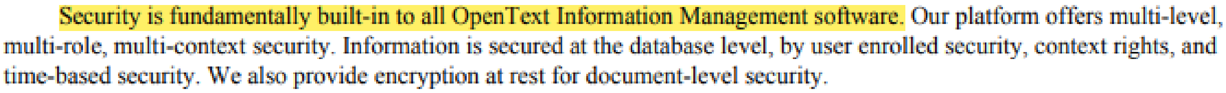

Endpoint Detection & Response (EDR)
Endpoint and Network Security
Digital Investigations and Forensics
Information Governance, Risk & Compliance
Data Protection, Backup and Migration
Threat Intelligence Services

Endpoint and Network Security

Go beyond traditional antivirus to keep critical systems, data and users safe from ransomware, phishing, malware and other cyberattacks with cyber security purpose-built for SMBs and home users.

- ✓ Webroot Business Endpoint Protection →
- ✓ Webroot DNS Protection →
- ✓ Webroot Security Awareness Training →
- ✓ Webroot SecureAnywhere AntiVirus for Home →

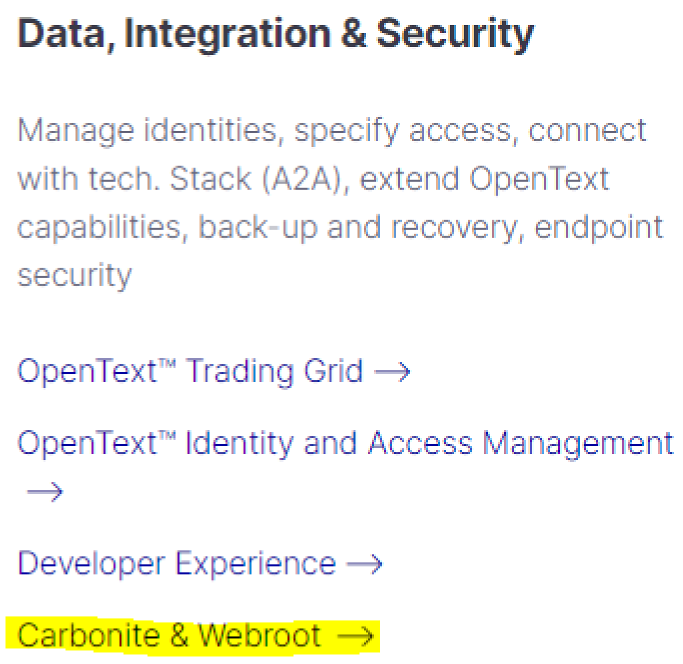
21. On information and belief, all of Open Text's security products including, but not limited to, Webroot products and Open Text Security, including OpenText EnCase, integrate with the rest of Open Text's product offerings. For example, Open Text states in its 2021 Annual Report that "[s]ecurity is fundamentally built-in to all OpenText Information Management software."



Security is fundamentally built-in to all OpenText Information Management software. Our platform offers multi-level, multi-role, multi-context security. Information is secured at the database level, by user enrolled security, context rights, and time-based security. We also provide encryption at rest for document-level security.

(https://s23.q4cdn.com/197378439/files/doc_financials/2021/ar/OpenText-2021-Annual-Report.pdf at pg. 8).

22. On information and belief, this "security" includes Webroot's security software, systems, and services. For example, Open Text uses Webroot's security software, systems, and services to provide security for its OpenText Experience Cloud.



Data, Integration & Security

Manage identities, specify access, connect with tech. Stack (A2A), extend OpenText capabilities, back-up and recovery, endpoint security

OpenText™ Trading Grid →

OpenText™ Identity and Access Management →

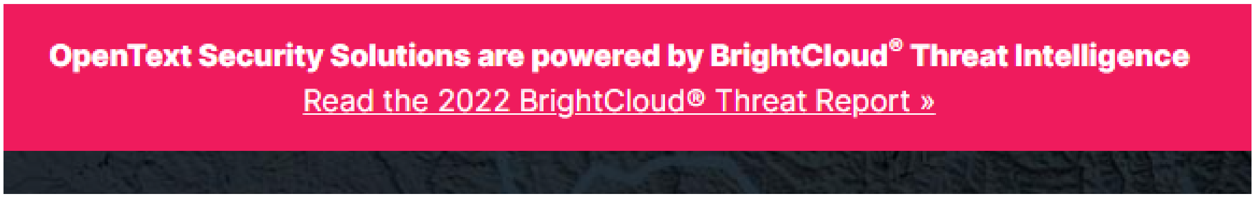
Developer Experience →

Carbonite & Webroot →

(https://www.opentext.com/products-and-solutions/products/digital-experience).

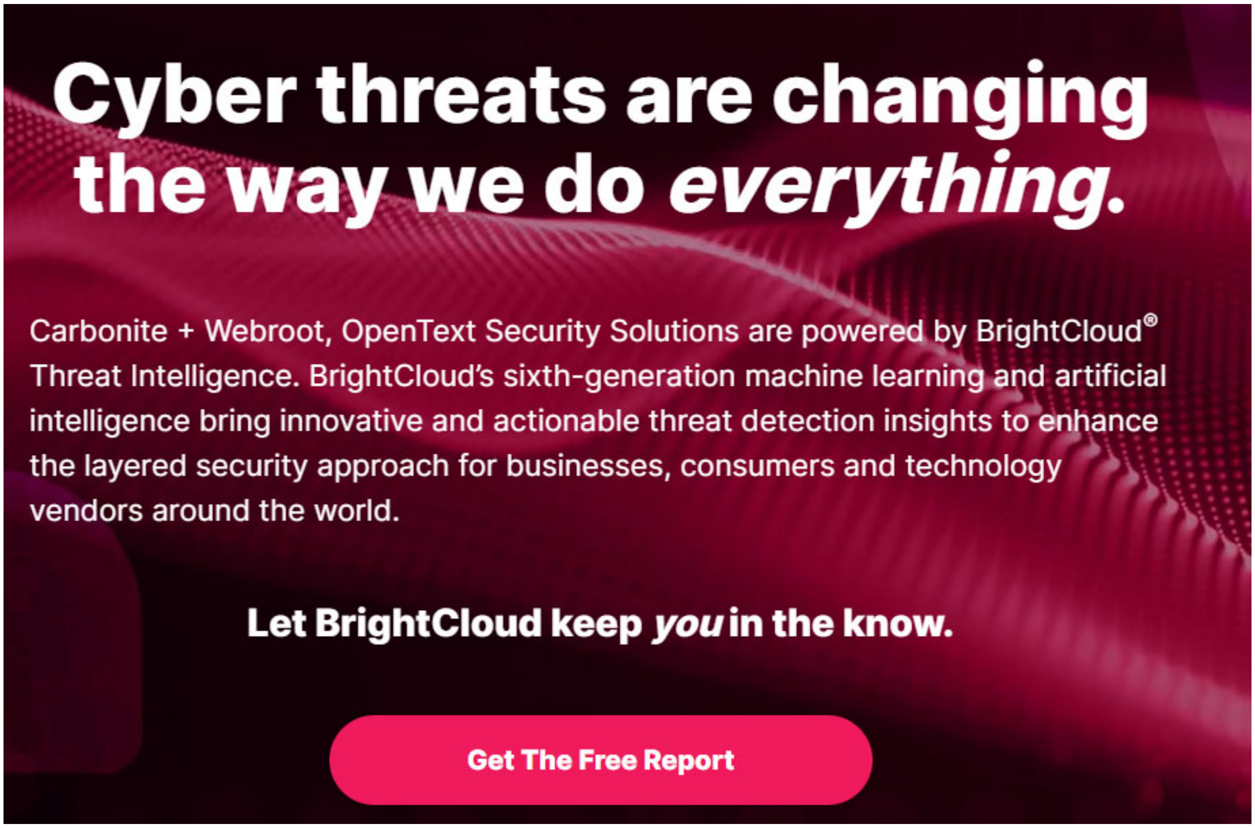
23. On information and belief, the security built-in to all OpenText Information Management software also includes OpenText's own security software, such as OpenText Security Solutions.

24. Furthermore, Open Text's security products, such as OpenText Security Solutions, are powered by BrightCloud Threat Intelligence, a Webroot product.



OpenText Security Solutions are powered by BrightCloud® Threat Intelligence
Read the 2022 BrightCloud® Threat Report »

(https://www.brightcloud.com/);

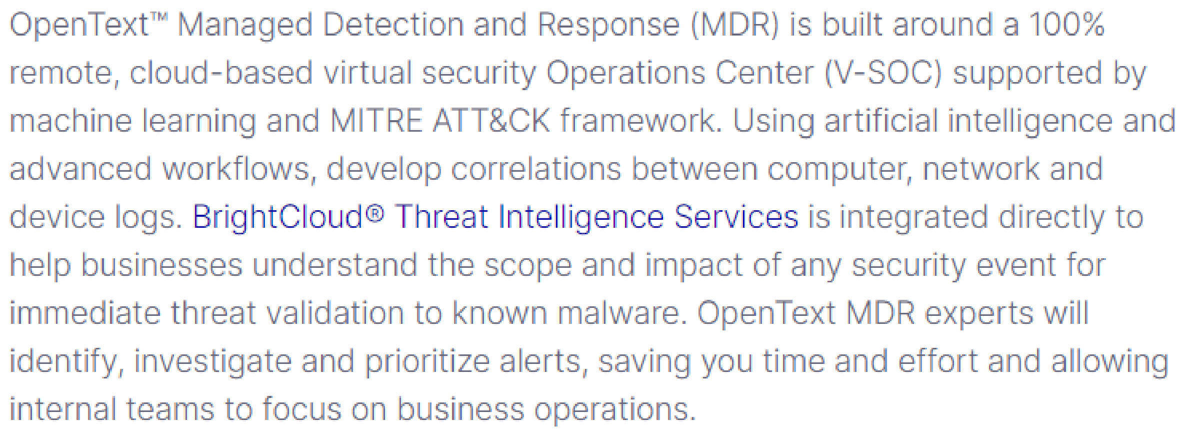


Cyber threats are changing the way we do *everything.*

Carbonite + Webroot, OpenText Security Solutions are powered by BrightCloud® Threat Intelligence. BrightCloud's sixth-generation machine learning and artificial intelligence bring innovative and actionable threat detection insights to enhance the layered security approach for businesses, consumers and technology vendors around the world.

Let BrightCloud keep *you* in the know.

(https://www.brightcloud.com/land/2022-brightcloud-threat-report);



OpenText™ Managed Detection and Response (MDR) is built around a 100% remote, cloud-based virtual security Operations Center (V-SOC) supported by machine learning and MITRE ATT&CK framework. Using artificial intelligence and advanced workflows, develop correlations between computer, network and device logs. BrightCloud® Threat Intelligence Services is integrated directly to help businesses understand the scope and impact of any security event for immediate threat validation to known malware. OpenText MDR experts will identify, investigate and prioritize alerts, saving you time and effort and allowing internal teams to focus on business operations.

(https://security.opentext.com/solutions/managed-detection-and-response).

25. The evidence above is exemplary of the fact that Webroot's security software, systems, and services and OpenText's security software, systems, and services are integrated with each Open Text product.

26. The Webroot Accused Products and Open Text Accused Products are collectively the "Accused Products."

COUNTERCLAIM ONE

(INFRINGEMENT OF U.S. PATENT NO. 8,838,992)

27. Trend Micro re-alleges and incorporates by reference each allegation contained in the preceding paragraphs of the Counterclaims.

28. Trend Micro is the lawful owner of all right, title, and interest in U.S. Patent No. 8,838,992 (the "'992 patent"), titled "Identification of normal scripts in computer systems," including the right to sue and to recover for any and all infringement thereof. The '992 patent was duly and legally issued on September 16, 2014 by the United States Patent and Trademark Office. A true and accurate copy of the '992 patent is attached hereto as Exhibit A.

29. The '992 Patent is valid and enforceable.

30. The '992 patent describes and claims inventive and patentable subject matter that provide a technological solution to a problem rooted in computer technology, and significantly improving on traditional methods of identifying malicious computer scripts.

31. Scripts, such as JavaScript, were commonly employed to enhance a user's web browsing experience. Websites would deliver these scripts with web pages to add functionality and features. However, scripts can also be used to exploit web browser or plug-in vulnerabilities. Thus, there was a need for techniques to combat malicious scripts.

32. Traditional anti-malware solutions analyzed all scripts performed on a computer to determine whether they were malicious or not. This was computationally resource-intensive because many of these scripts were encrypted so they had to be decrypted or emulated to analyze. Emulating and decrypting scripts at this rate was inefficient because less than 0.1% of

scripts received over the internet were actually malicious. But there was still a need to screen scripts in order to guard against the occasional malicious script.

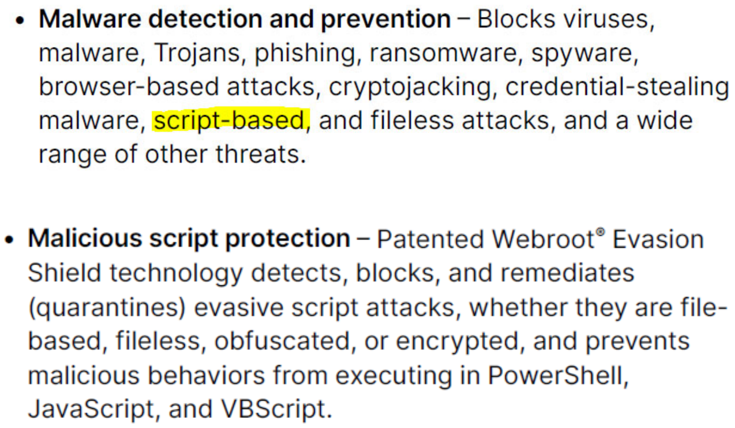
33. The '992 patent improved on prior art anti-malware solutions by providing a much more efficient solution to guard against malicious scripts. Instead of emulating and decrypting every script run by a website, the patent claims an invention that determines whether a script is either normal or potentially malicious using machine learning. By performing lexical semantic analysis on scripts using a machine learning model, scripts could be identified as normal or potentially malicious without having to decrypt or emulate the script, thereby significantly reducing the amount of computational resources required to detect malicious scripts. For example claim 1 recites:

> 1. A computer-implemented method of identifying normal scripts, the method comprising:
>
> receiving a machine learning model and a feature set in a client computer, the machine learning model being trained using sample scripts that are known to be normal and sample scripts that are known to be potentially malicious and takes into account lexical and semantic characteristics of the sample scripts that are known to be normal and the sample scripts that are known to be potentially malicious;
>
> receiving a target script along with a web page in the client computer, the target script and the web page being received from a server computer over a computer network; extracting from the target script features that are included in the feature set;
>
> inputting the extracted features of the target script into the machine learning model to receive a classification of the target script from the machine learning model; and
>
> detecting that the target script is a normal script and not a potentially malicious script based on the classification of the target script.

34. Counter-Defendants Webroot and Open Text have infringed and continue to infringe one or more claims of the '992 patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a) at least by, without authority, making, using, offering to sell, and/or selling within the United States the Accused Products.

35. For example, Counter-Defendants Webroot and Open Text have directly infringed at least claim 1 through their use and operation of the Accused Products, including through the execution of software that has been designed and built by Open Text and Webroot to perform each of the steps of claim 1. On information and belief, Open Text and Webroot also perform the steps of claim 1 when testing the operation of the Accused Products. A non-limiting example of Open Text's and Webroot's infringement of claim 1 is described below with respect to Webroot SecureAnywhere Business Endpoint Protection.

36. To the extent the preamble is limiting, Webroot and Open Text perform *a computer-implemented method of identifying normal scripts.* For example, Webroot SecureAnywhere Business Endpoint Protection is a computer service that integrates with BrightCloud Threat Intelligence Services, also run by Webroot and Open Text, to classify files and processes, including scripts, as good or bad.



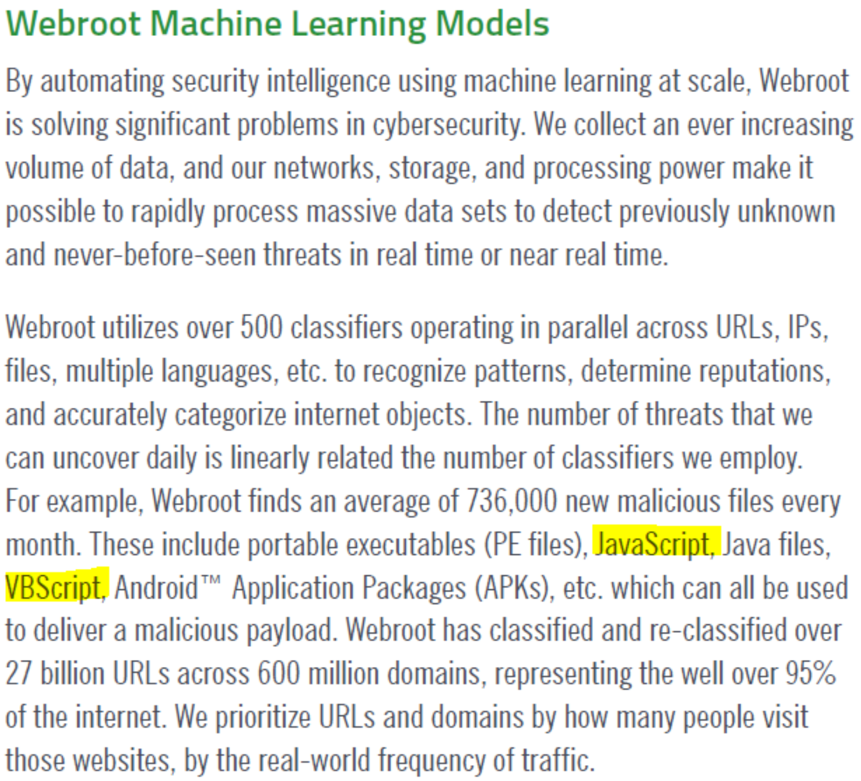
- **Malware detection and prevention** – Blocks viruses, malware, Trojans, phishing, ransomware, spyware, browser-based attacks, cryptojacking, credential-stealing malware, script-based, and fileless attacks, and a wide range of other threats.

- **Malicious script protection** – Patented Webroot® Evasion Shield technology detects, blocks, and remediates (quarantines) evasive script attacks, whether they are file-based, fileless, obfuscated, or encrypted, and prevents malicious behaviors from executing in PowerShell, JavaScript, and VBScript.

https://www-cdn.webroot.com/2116/0987/5719/Webroot_Endpoint_Protection_DS_us.pdf

("Business Endpoint Protection Datasheet") at 2.

37. Furthermore, Webroot states that SecureAnywhere Business Endpoint Protection products uses a machine learning model that classifies various scripts as threats.

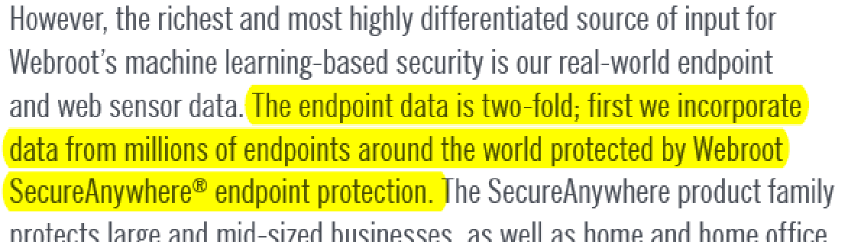


Webroot Machine Learning Models

By automating security intelligence using machine learning at scale, Webroot is solving significant problems in cybersecurity. We collect an ever increasing volume of data, and our networks, storage, and processing power make it possible to rapidly process massive data sets to detect previously unknown and never-before-seen threats in real time or near real time.

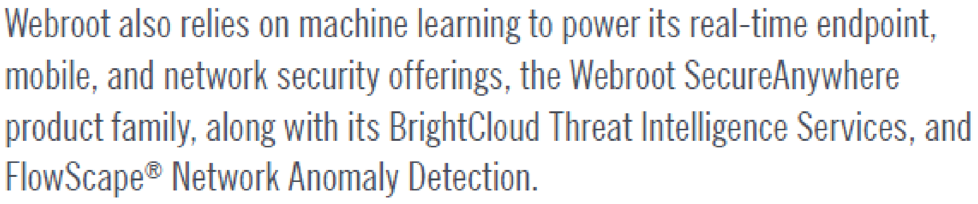
Webroot utilizes over 500 classifiers operating in parallel across URLs, IPs, files, multiple languages, etc. to recognize patterns, determine reputations, and accurately categorize internet objects. The number of threats that we can uncover daily is linearly related the number of classifiers we employ. For example, Webroot finds an average of 736,000 new malicious files every month. These include portable executables (PE files), JavaScript, Java files, VBScript, Android™ Application Packages (APKs), etc. which can all be used to deliver a malicious payload. Webroot has classified and re-classified over 27 billion URLs across 600 million domains, representing the well over 95% of the internet. We prioritize URLs and domains by how many people visit those websites, by the real-world frequency of traffic.

https://www-cdn.webroot.com/1215/2510/8234/Machine-Learning-Webroot-Approach-WP_US.pdf ("Webroot Machine Learning Whitepaper") at 2;



However, the richest and most highly differentiated source of input for Webroot's machine learning-based security is our real-world endpoint and web sensor data. The endpoint data is two-fold; first we incorporate data from millions of endpoints around the world protected by Webroot SecureAnywhere® endpoint protection. The SecureAnywhere product family protects large and mid-sized businesses, as well as home and home office

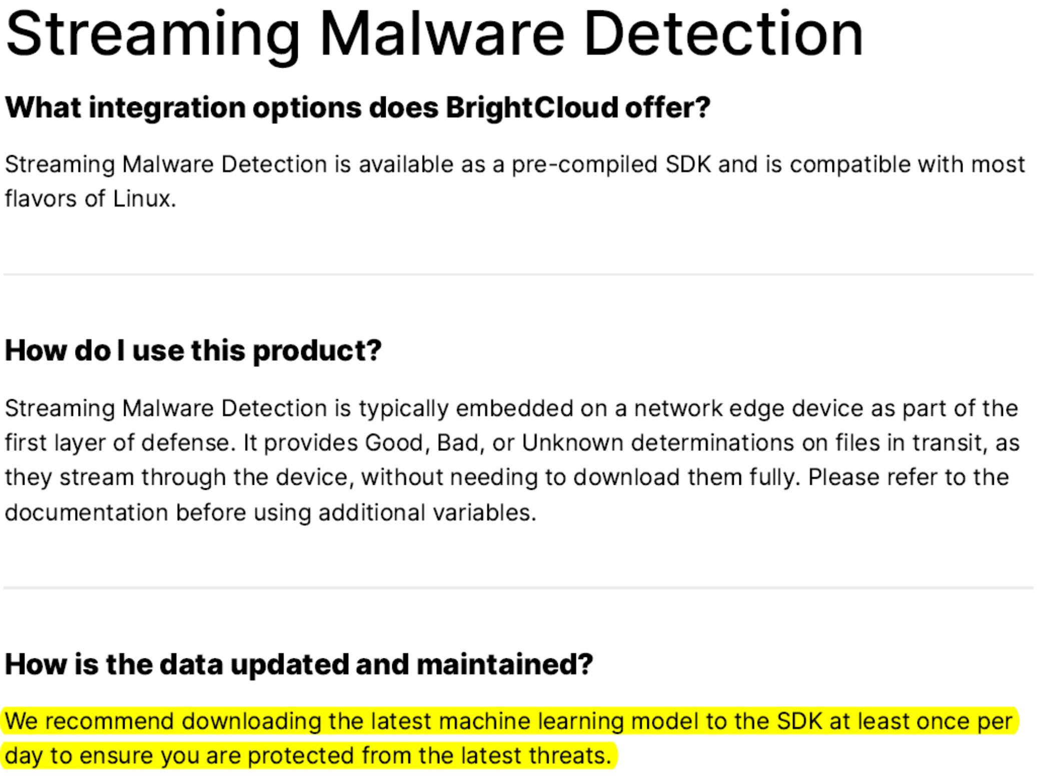
Id. at 3;



Webroot also relies on machine learning to power its real-time endpoint, mobile, and network security offerings, the Webroot SecureAnywhere product family, along with its BrightCloud Threat Intelligence Services, and FlowScape® Network Anomaly Detection.

Id. at 4.

38. Webroot and Open Text perform the step of "*receiving a machine learning model and a feature set in a client computer, the machine learning model being trained using sample scripts that are known to be normal and sample scripts that are known to be potentially malicious and takes into account lexical and semantic characteristics of the sample scripts that are known to be normal and the sample scripts that are known to be potentially malicious*." As explained above, Webroot SecureAnywhere Business Endpoint Protection integrates with BrightCloud Threat Intelligence. BrightCloud Threat Intelligence encompasses BrightCloud Streaming Malware Detection, which uses a machine learning model and feature set that is downloaded to a client computer.



Streaming Malware Detection

What integration options does BrightCloud offer?

Streaming Malware Detection is available as a pre-compiled SDK and is compatible with most flavors of Linux.

How do I use this product?

Streaming Malware Detection is typically embedded on a network edge device as part of the first layer of defense. It provides Good, Bad, or Unknown determinations on files in transit, as they stream through the device, without needing to download them fully. Please refer to the documentation before using additional variables.

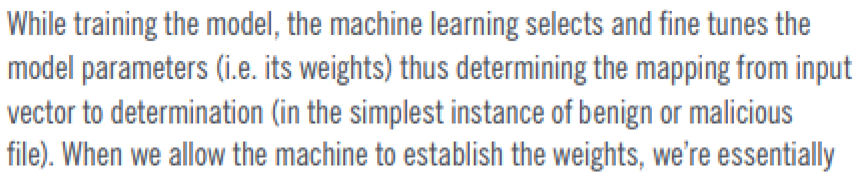
How is the data updated and maintained?

We recommend downloading the latest machine learning model to the SDK at least once per day to ensure you are protected from the latest threats.

https://www.brightcloud.com/faq.

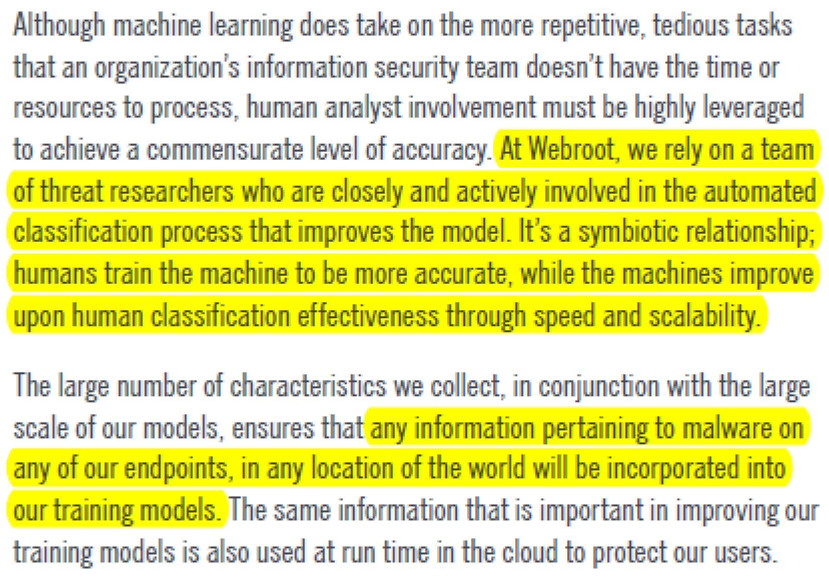
39. BrightCloud Threat Intelligence trains machine learning models using training samples, including scripts, that are known to be benign (normal) and training samples, including

scripts, that are known to be potentially malicious. On information and belief, Webroot SecureAnywhere Business Endpoint Protection, which integrates with BrightCloud Threat Intelligence, utilizes BrightCloud Threat Intelligence's trained machine learning model to detect potentially malicious scripts.



While training the model, the machine learning selects and fine tunes the model parameters (i.e. its weights) thus determining the mapping from input vector to determination (in the simplest instance of benign or malicious file). When we allow the machine to establish the weights, we're essentially

Webroot Machine Learning Whitepaper at 3;

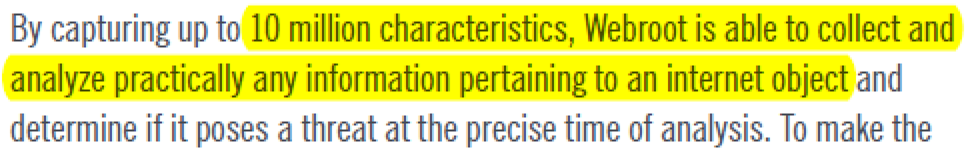


Although machine learning does take on the more repetitive, tedious tasks that an organization's information security team doesn't have the time or resources to process, human analyst involvement must be highly leveraged to achieve a commensurate level of accuracy. At Webroot, we rely on a team of threat researchers who are closely and actively involved in the automated classification process that improves the model. It's a symbiotic relationship; humans train the machine to be more accurate, while the machines improve upon human classification effectiveness through speed and scalability.

The large number of characteristics we collect, in conjunction with the large scale of our models, ensures that any information pertaining to malware on any of our endpoints, in any location of the world will be incorporated into our training models. The same information that is important in improving our training models is also used at run time in the cloud to protect our users.

id. at 4.

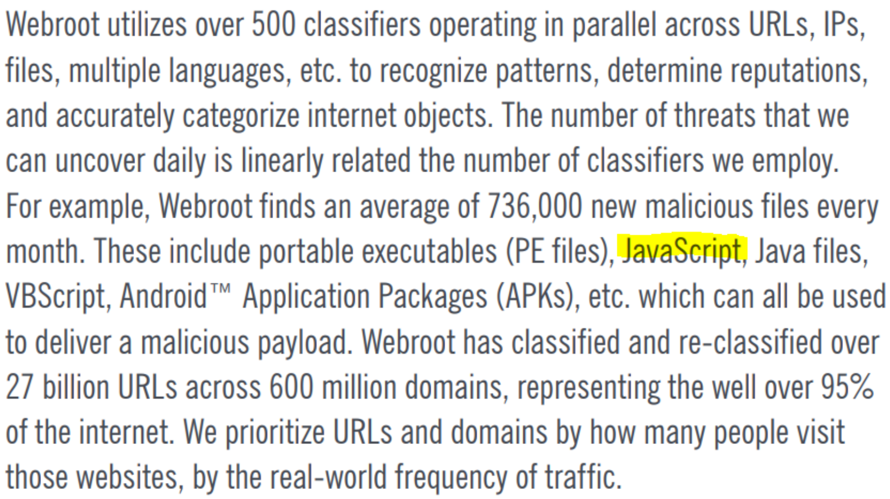
40. The BrightCloud Threat Intelligence machine learning model takes into account 10 million characteristics of the training samples, which comprises "practically any information pertaining to" the sample. On information and belief, this includes lexical and semantic characteristics of the training sample scripts.



By capturing up to 10 million characteristics, Webroot is able to collect and analyze practically any information pertaining to an internet object and determine if it poses a threat at the precise time of analysis. To make the

https://www-cdn.webroot.com/7616/4554/8137/BrightCloud_Threat_Intelligence_Services_DS_AMER_EN.pdf.Webroot.

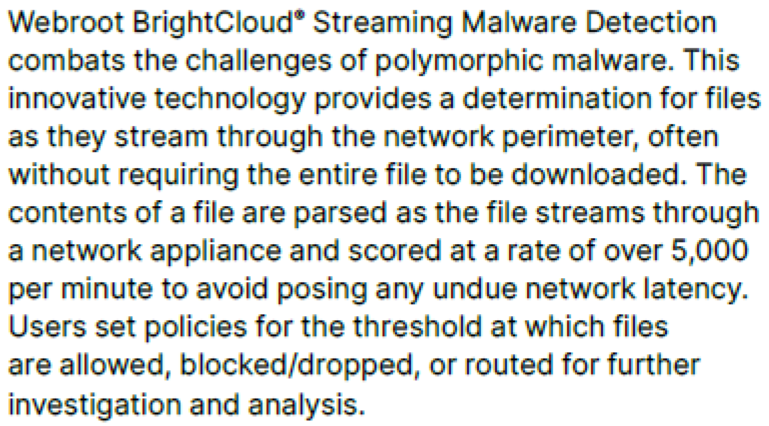
41. Webroot and Open Text perform the step of "*receiving a target script along with a web page in the client computer, the target script and the web page being received from a server computer over a computer network*." For example, Webroot's SecureAnywhere Business Endpoint Protection receives webpages that contain JavaScript from a server computer over a computer network.



Webroot utilizes over 500 classifiers operating in parallel across URLs, IPs, files, multiple languages, etc. to recognize patterns, determine reputations, and accurately categorize internet objects. The number of threats that we can uncover daily is linearly related the number of classifiers we employ. For example, Webroot finds an average of 736,000 new malicious files every month. These include portable executables (PE files), JavaScript, Java files, VBScript, Android™ Application Packages (APKs), etc. which can all be used to deliver a malicious payload. Webroot has classified and re-classified over 27 billion URLs across 600 million domains, representing the well over 95% of the internet. We prioritize URLs and domains by how many people visit those websites, by the real-world frequency of traffic.

"Webroot Machine Learning Whitepaper" at 2.

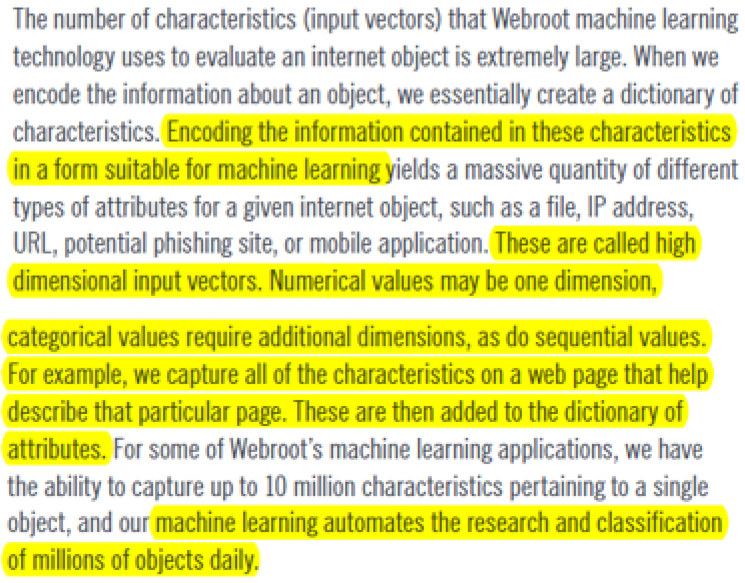
42. Further, BrightCloud Threat Intelligence's Streaming Malware Detection analyzes files, such as a script and the webpage in which it is found, as they stream through the network perimeter.



Webroot BrightCloud® Streaming Malware Detection combats the challenges of polymorphic malware. This innovative technology provides a determination for files as they stream through the network perimeter, often without requiring the entire file to be downloaded. The contents of a file are parsed as the file streams through a network appliance and scored at a rate of over 5,000 per minute to avoid posing any undue network latency. Users set policies for the threshold at which files are allowed, blocked/dropped, or routed for further investigation and analysis.

https://www-cdn.webroot.com/1516/0987/5232/Webroot_BrightCloud_Streaming_Malware_Detection_DS.pdf at 1.

43. Webroot and Open Text perform the step of "*extracting from the target script features that are included in the feature set.*" Webroot SecureAnywhere Business Endpoint Protection extracts features included in the feature set from internet objects such as scripts.

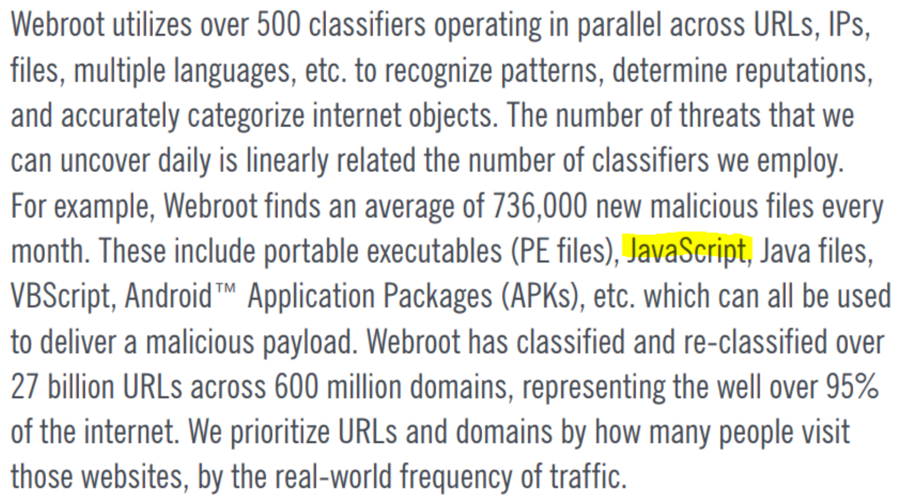


The number of characteristics (input vectors) that Webroot machine learning technology uses to evaluate an internet object is extremely large. When we encode the information about an object, we essentially create a dictionary of characteristics. Encoding the information contained in these characteristics in a form suitable for machine learning yields a massive quantity of different types of attributes for a given internet object, such as a file, IP address, URL, potential phishing site, or mobile application. These are called high dimensional input vectors. Numerical values may be one dimension, categorical values require additional dimensions, as do sequential values. For example, we capture all of the characteristics on a web page that help describe that particular page. These are then added to the dictionary of attributes. For some of Webroot's machine learning applications, we have the ability to capture up to 10 million characteristics pertaining to a single object, and our machine learning automates the research and classification of millions of objects daily.

Webroot Machine Learning Whitepaper at 2.

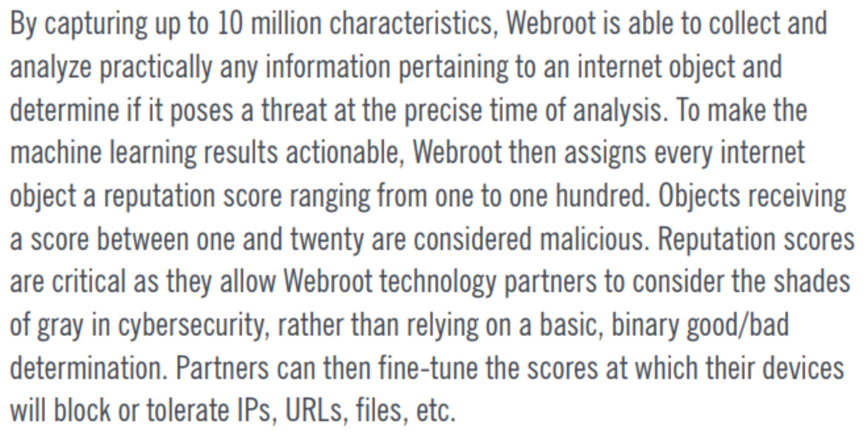
44. Webroot and Open Text perform the step of "*inputting the extracted features of*

the target script into the machine learning model to receive a classification of the target script from the machine learning model." Webroot SecureAnywhere Business Endpoint Protection inputs the extracted features of the target script into the machine learning model to receive a classification of the target script from the machine learning model.



Webroot utilizes over 500 classifiers operating in parallel across URLs, IPs, files, multiple languages, etc. to recognize patterns, determine reputations, and accurately categorize internet objects. The number of threats that we can uncover daily is linearly related the number of classifiers we employ. For example, Webroot finds an average of 736,000 new malicious files every month. These include portable executables (PE files), JavaScript, Java files, VBScript, Android™ Application Packages (APKs), etc. which can all be used to deliver a malicious payload. Webroot has classified and re-classified over 27 billion URLs across 600 million domains, representing the well over 95% of the internet. We prioritize URLs and domains by how many people visit those websites, by the real-world frequency of traffic.

"Webroot Machine Learning Whitepaper" at 2;

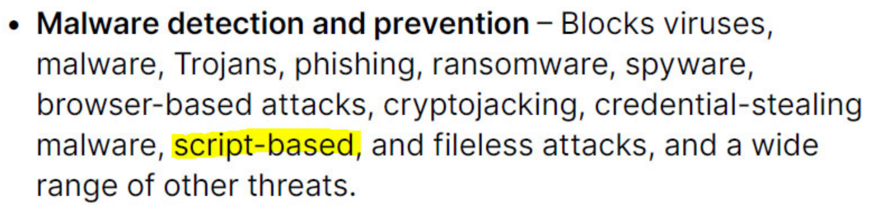


By capturing up to 10 million characteristics, Webroot is able to collect and analyze practically any information pertaining to an internet object and determine if it poses a threat at the precise time of analysis. To make the machine learning results actionable, Webroot then assigns every internet object a reputation score ranging from one to one hundred. Objects receiving a score between one and twenty are considered malicious. Reputation scores are critical as they allow Webroot technology partners to consider the shades of gray in cybersecurity, rather than relying on a basic, binary good/bad determination. Partners can then fine-tune the scores at which their devices will block or tolerate IPs, URLs, files, etc.

id.

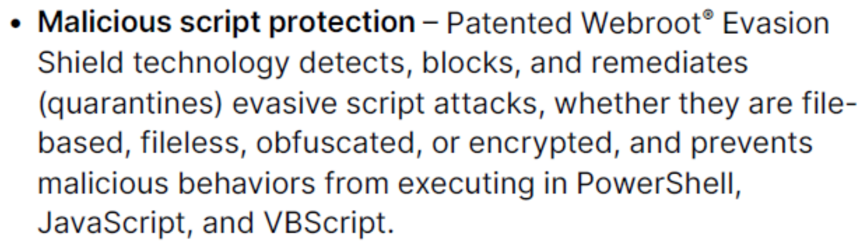
45. Webroot and Open Text perform the step of "*detecting that the target script is a normal script and not a potentially malicious script based on the classification of the target script.*" Webroot SecureAnywhere Business Endpoint Protection detects whether the script is

normal or potentially malicious based on the classification.



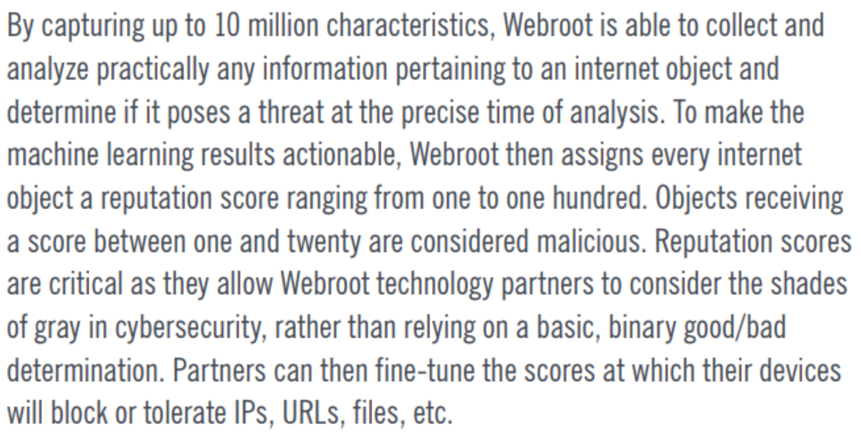
- **Malware detection and prevention** – Blocks viruses, malware, Trojans, phishing, ransomware, spyware, browser-based attacks, cryptojacking, credential-stealing malware, script-based, and fileless attacks, and a wide range of other threats.

Business Endpoint Protection Datasheet at 2;



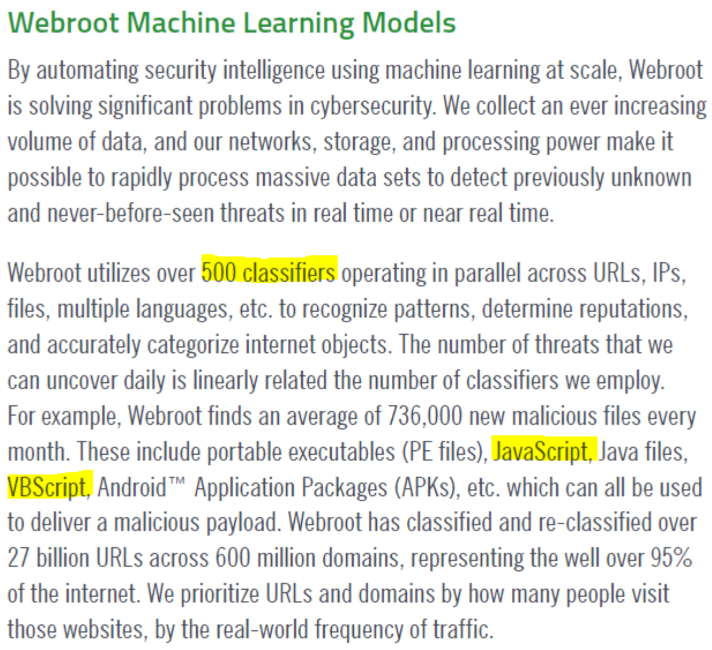
- **Malicious script protection** – Patented Webroot® Evasion Shield technology detects, blocks, and remediates (quarantines) evasive script attacks, whether they are file-based, fileless, obfuscated, or encrypted, and prevents malicious behaviors from executing in PowerShell, JavaScript, and VBScript.

id.;



By capturing up to 10 million characteristics, Webroot is able to collect and analyze practically any information pertaining to an internet object and determine if it poses a threat at the precise time of analysis. To make the machine learning results actionable, Webroot then assigns every internet object a reputation score ranging from one to one hundred. Objects receiving a score between one and twenty are considered malicious. Reputation scores are critical as they allow Webroot technology partners to consider the shades of gray in cybersecurity, rather than relying on a basic, binary good/bad determination. Partners can then fine-tune the scores at which their devices will block or tolerate IPs, URLs, files, etc.

Webroot Machine Learning Whitepaper at 2;



Webroot Machine Learning Models

By automating security intelligence using machine learning at scale, Webroot is solving significant problems in cybersecurity. We collect an ever increasing volume of data, and our networks, storage, and processing power make it possible to rapidly process massive data sets to detect previously unknown and never-before-seen threats in real time or near real time.

Webroot utilizes over 500 classifiers operating in parallel across URLs, IPs, files, multiple languages, etc. to recognize patterns, determine reputations, and accurately categorize internet objects. The number of threats that we can uncover daily is linearly related the number of classifiers we employ. For example, Webroot finds an average of 736,000 new malicious files every month. These include portable executables (PE files), JavaScript, Java files, VBScript, Android™ Application Packages (APKs), etc. which can all be used to deliver a malicious payload. Webroot has classified and re-classified over 27 billion URLs across 600 million domains, representing the well over 95% of the internet. We prioritize URLs and domains by how many people visit those websites, by the real-world frequency of traffic.

id.

46. The above description is based on publicly available information and a reasonable investigation of the operation of the Accused Products. Trend Micro reserves the right to modify this description, including, for example, on the basis of information about the Accused Products that it obtains during discovery.

47. Counter-Defendants Open Text and Webroot became aware of the ‘992 patent at least as of the filing of Trend Micro’s Counterclaims on May 16, 2022.

48. To the extent the marking requirement applies with respect to the ’992 patent, Trend Micro has a practice of marking at least its product manuals with the patents that the product practices.

49. Counter-Defendants Open Text and Webroot and their partners, customers, and end users of its Accused Products and corresponding systems and services, directly infringe at least claim 1 of the ‘992 patent, literally or under the doctrine of equivalents, at least by using the Accused Products as described above. On information and belief, the infringing actions of

Open Text's and Webroot's partners, customers, and end users of the Accused Products are attributable to Open Text and Webroot. For example, Open Text and Webroot direct and control their partners by contractual agreement to operate, or to provide Open Text and Webroot with the means to operate (*e.g.*, servers), or otherwise distribute the Accused Products in a manner that infringes the '992 patent. Open Text and Webroot further condition receipt of benefit of the Accused Products upon use of the patented features, such as performing steps of the methods claimed in the '992 patent.

50. In addition to Counter-Defendants Open Text's and Webroot's and their customers' direct infringement, Open Text and Webroot have infringed and continue to infringe the '992 patent indirectly, including by actively inducing others to directly infringe at least claim 1 of the '992 patent in violation of 35 U.S.C. § 271(b).

51. For example, Open Text and Webroot encourage and induce customers to use the Accused Products in a manner that infringes claim 1 of the '992 patent by at least offering and providing software that performs a method that infringes claim 1 when installed and operated by the customers, and by activities related to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

52. Open Text and Webroot encourage and induce third parties to use the Accused Products in a manner that infringes the '992 patent as described above , including through advertising, marketing, customer support, user manuals, instructions, installation, and distribution of the Accused Products in the United States. For example, Counter-Defendants' customers and end users test and/or operate Webroot SecureAnywhere in the United States in accordance with Counter-Defendants' instructions contained in, for example, its user manuals, thereby also performing the claimed methods and infringing the asserted claims of the '992

Patent reciting such operation. *See* Webroot Machine Learning Whitepaper; Business Endpoint Protection Datasheet.

53. Moreover, Open Text and Webroot contribute to infringement of the ’992 patent by, among other activities, making, using, offering for sale, selling within the United States, and/or importing into the United States the Accused Products with knowledge that such activities practice every element of one or more claims of the ’992 patent, or being willfully blind to such activities practicing every element of one or more claims of the ’992 patent. Counter-Defendants’ affirmative acts of making, offering for sale, selling, and/or importing into the United States the Accused Products contribute to Counter-Defendants’ customers and end-users infringing of the Accused Products. The infringing software components of the Accused Products are specially designed in a way that infringes one or more claims of the ’992 patent and can be used only in a manner that infringes the ’992 patent and thus have no substantial non-infringing uses.

54. The above description regarding Counter-Defendants’ infringement of the ’992 patent is based on publicly available information and a reasonable investigation of the operation of the Accused Products. Trend Micro reserves the right to modify this description, including, for example, on the basis of information about the Accused Products that it obtains during discovery.

55. Unless and until enjoined by this Court, Counter-Defendants will continue to infringe the ’992 patent. Counter-Defendants Open Text’s and Webroot’s infringement is causing and will continue to cause Trend Micro irreparable harm, for which there is no remedy at law.

56. Under 35 U.S.C. § 283, Trend Micro is entitled to a preliminary and permanent

injunction against further infringement of the ’992 patent.

57. Counter-Defendants’ infringement of the ’992 patent has been knowing and willful since at least the filing of Trend Micro’s Counterclaims on May 16, 2022.

58. Trend Micro has suffered and continues to suffer damages, including lost profits, as a result of Counter-Defendants Open Text’s and Webroot’s infringement of the ‘992 patent. Under 35 U.S.C. § 284, Trend Micro is entitled to damages adequate to compensate it for Counter-Defendants Open Text’s and Webroot’s infringement, in no event less than a reasonable royalty for Counter-Defendants’ use of the inventions of the ’992 patent, together with interest and costs as fixed by the Court.

COUNTERCLAIM TWO

(INFRINGEMENT OF U.S. PATENT NO. 8,051,487)

59. Trend Micro incorporates by reference its responses contained in the foregoing paragraphs, as if fully set forth herein.

60. Trend Micro is the lawful owner of all right, title, and interest in U.S. Patent No. 8,051,487 (the “’487 patent”), titled “Cascading security architecture,” including the right to sue and to recover for any and all infringement thereof. The ’487 patent was duly and legally issued on November 11, 2011 by the United States Patent and Trademark Office. A true and accurate copy of the ’487 patent is attached hereto as Exhibit B.

61. The ’487 patent is valid and enforceable.

62. The ’487 patent describes and claims inventive and patentable subject matter that provide a technological solution to a problem rooted in computer technology, and significantly improves on traditional methods and apparatuses for managing enterprise documents with sensitive information at an endpoint of a system.

63. Documents containing highly sensitive information were traditionally stored in an isolated and secured computer, accessible only to authorized personals who followed "a secure administration procedure (or policy) to prevent unauthorized access." '487 patent at 1:62-67. However, "conventional isolation-type security techniques are not reliable, since the access control relies upon people following the secure administration procedure," and the "administration procedure is difficult to manage with respect to education and enforcement of such security policies, and also can be quite costly to implement and monitor." '487 patent at 2:5-10. Various conventional approaches to prevent sensitive information leakage from endpoints had their own limits, such as lack of "deep inspection of the document content," inability to "prevent sensitive information leakage caused by intentional scrambling of sensitive documents," "difficulty in maintaining and managing different users and their corresponding privileges," inability to "analyze encrypted network traffic," and slow data transmission. '487 patent at 2:11-47. The '487 patent solves these limits by proposing a method for detecting and tracking documents with sensitive information in the endpoints of a system or sensitive documents being exported out of the endpoints of the system. '487 patent at 2:56-43. By detecting documents in motion and determining whether a document is sensitive based on its content and user behavior, detection of a sensitive document is likely to be complete and accurate. '487 patent at 3:21-26. By analyzing user behavior based on activity-to-behavior patterns, intentional data scrambling can be detected and an appropriate cause of action may be taken relative to the detected document. '487 patent at 3:26-29. Further, because most of the document management is achieved in the endpoint, the system can prevent leakage of sensitive information from the endpoint even when the endpoint is disconnected from the enterprise network. '487 patent at 3:30-34.

64. For example, claim 1 of the ’487 patent recites:

> 1. A method for managing documents with sensitive information at an endpoint of a system, the method comprising:
>
> identifying, by an agent configured as software elements programmed to run on a computing device, a target document and an associated current process activity, wherein the associated current process activity comprises an operation to be performed on the target document;
>
> determining, by the agent, whether the target document is an outgoing document which is a document that is to be exported out of the endpoint;
>
> if the target document is determined to not be an outgoing document, then identifying, by the agent, a behavior applied to the target document;
>
> determining, by the agent, whether the target document contains sensitive information; and
>
> responsive to the target document containing the sensitive information, the agent determining whether the current process activity is to be blocked allowed or modified,
>
> wherein after the agent identifies the target document and the associated current process activity, the agent holds the current process activity, notifies a behavior analysis engine of the target document and the current process activity, and waits for a signal from the behavior analysis engine indicating whether to continue with the current process activity,
>
> wherein the agent raises an exception and stops the current process activity if the agent is signaled by the behavior analysis engine to block the current process activity, otherwise the agent lets the current process activity to continue.

65. Counter-Defendant Open Text has infringed and continue to infringe one or more claims of the ’487 patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a) at least by, without authority, making, using, offering to sell, and/or selling within the United States infringing products and services such as OpenText enterprise content management solutions, including but not limited to, OpenText eDOCS and other products and

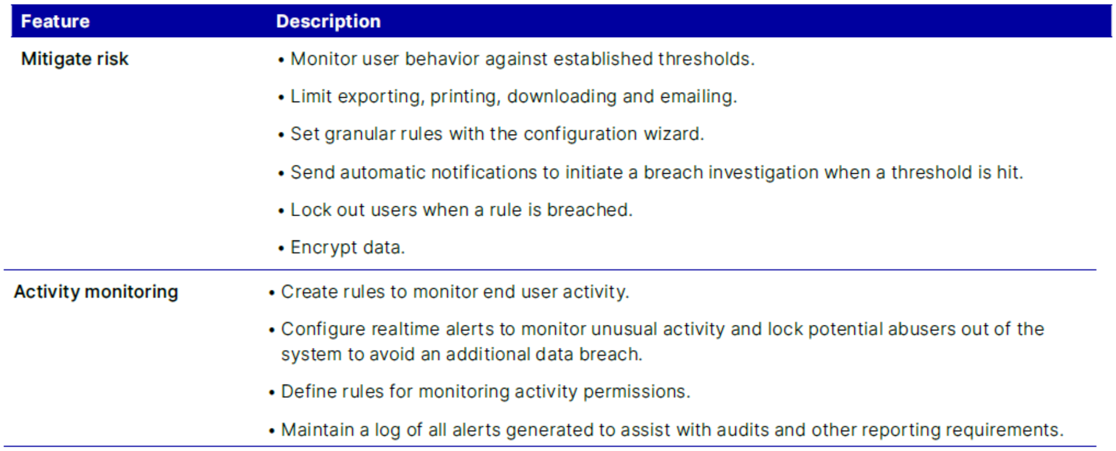
solutions utilizing the OpenText eDOCS platform. (collectively, the "'487 Accused Products").

66. For example, Counter-Defendant Open Text has directly infringed at least claim 1 of the '487 patent through its use and operation of the '487 Accused Products, including through the execution of software that has been designed and built by Open Text to perform each of the steps of claim 1. On information and belief, Open Text also performs the steps of claim 1 when testing the operation of the '487 Accused Products. A non-limiting example of Open Text's infringement of claim 1 is described below with respect to Open Text eDOCS.

67. To the extent the preamble is limiting, Open Text performs "*a method for managing documents with sensitive information at an endpoint of a system*." For example, OpenText eDOCS provides a method for managing documents with sensitive information at an endpoint of a system. Specifically, OpenText eDOCS uses eDOCS Defense, which is a document security module for preventing the leak of sensitive information through an internal security breach. *See* https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-edocs-defense-data-sheet-en.pdf ("OpenText eDOCS Defense Data Sheet") at 1 ("With eDOCS Defense, organizations can send templated alerts before and after sensitive information has been locked down, to further mitigate the risk and cost of a data breach, even safeguarding information from authorized users. As alerts are flexible and configurable, they can be sent to designated individuals at various stages of a potential breach, for example at 50 percent, 80 percent or 90 percent. These warnings can pre-empt a breach, lock out a user when they breach a rule, limit damage and, with stored system logs, can help organizations easily meet required regulations.").

68. Open Text performs the step of "*identifying, by an agent configured as software elements programmed to run on a computing device, a target document and an associated*

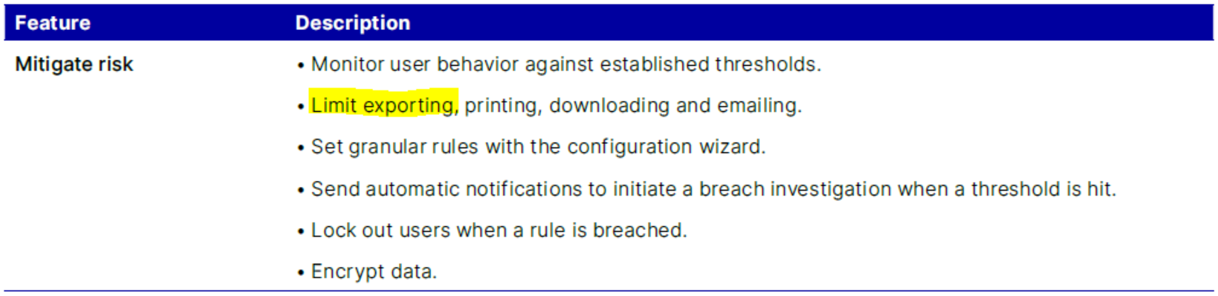
current process activity, wherein the associated current process activity comprises an operation to be performed on the target document." For example, OpenText eDOCS identifies a target document and an associated current process activity that comprises an operation to be performed on a target document. As an example, the description below shows that OpenText eDOCS Defense monitors for actions performed on a target document, such as exporting, printing, downloading, and emailing. On information and belief, such monitoring process is performed by an agent configured as software elements programmed to run on a computing device.



Feature	Description
Mitigate risk	• Monitor user behavior against established thresholds. • Limit exporting, printing, downloading and emailing. • Set granular rules with the configuration wizard. • Send automatic notifications to initiate a breach investigation when a threshold is hit. • Lock out users when a rule is breached. • Encrypt data.
Activity monitoring	• Create rules to monitor end user activity. • Configure realtime alerts to monitor unusual activity and lock potential abusers out of the system to avoid an additional data breach. • Define rules for monitoring activity permissions. • Maintain a log of all alerts generated to assist with audits and other reporting requirements.

See OpenText eDOCS Defense Data Sheet at 2.

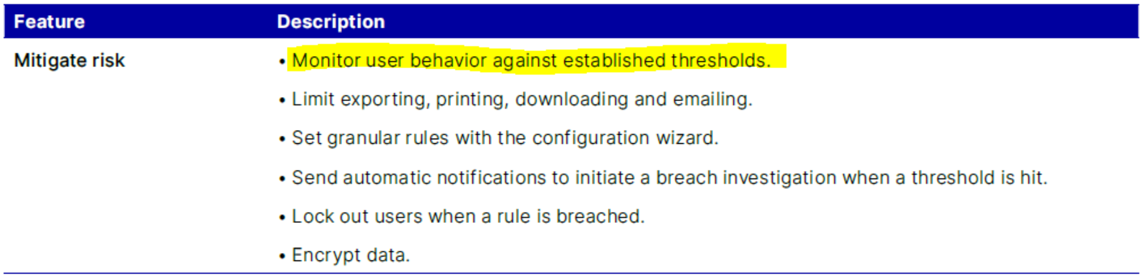
69. Open Text performs the step of "*determining, by the agent, whether the target document is an outgoing document which is a document that is to be exported out of the endpoint*." For example, OpenText eDOCS Defense determines by the agent whether the target document is an outgoing document which is a document that is to be exported out of the endpoint. As illustrated below, OpenText eDOCS Defense limits exporting.



Feature	Description
Mitigate risk	• Monitor user behavior against established thresholds. • Limit exporting, printing, downloading and emailing. • Set granular rules with the configuration wizard. • Send automatic notifications to initiate a breach investigation when a threshold is hit. • Lock out users when a rule is breached. • Encrypt data.

See OpenText eDOCS Defense Data Sheet at 2.

70. Open Text performs the step of "*if the target document is determined to not be an outgoing document, then identifying, by the agent, a behavior applied to the target document*." For example, if the target document is determined not to be an outgoing document, OpenText eDOCS Defense identifies by the agent a behavior applied to the target document. As illustrated below, OpenText eDOCs Defense monitors user behavior against established thresholds.



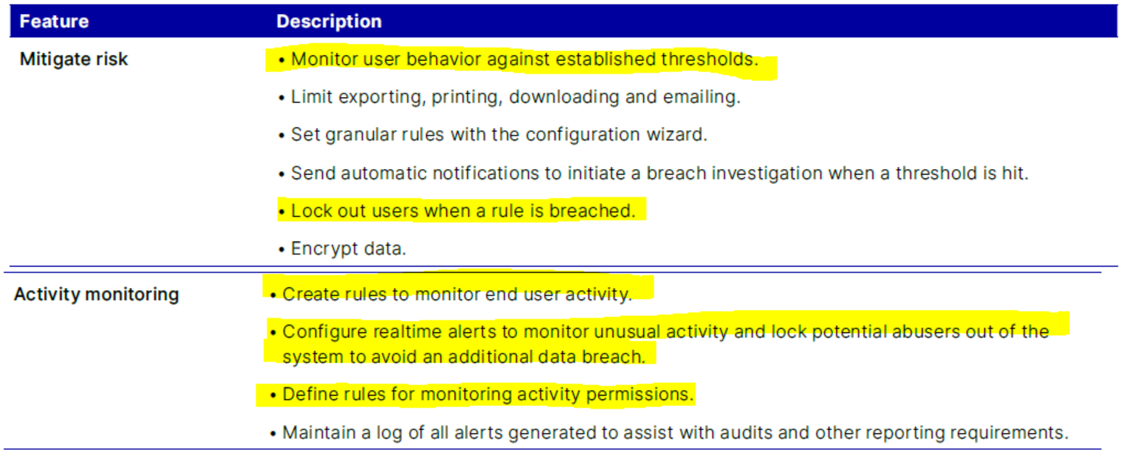
Feature	Description
Mitigate risk	• Monitor user behavior against established thresholds. • Limit exporting, printing, downloading and emailing. • Set granular rules with the configuration wizard. • Send automatic notifications to initiate a breach investigation when a threshold is hit. • Lock out users when a rule is breached. • Encrypt data.

See OpenText eDOCS Defense Data Sheet at 2.

71. Open Text performs the step of "*determining, by the agent, whether the target document contains sensitive information*." For example, OpenText eDOCS determines whether a document contains sensitive information. Specifically, OpenText eDOCS Defense specifically protects documents containing sensitive information. *See* OpenText eDOCS Defense Data Sheet at 1 ("With eDOCS Defense, organizations can send templated alerts before and after sensitive information has been locked down, to further mitigate the risk and cost of a data breach, even safeguarding information from authorized users. As alerts are flexible and configurable, they can be sent to designated individuals at various stages of a potential breach, for example at 50 percent, 80 percent or 90 percent. These warnings can pre-empt a breach, lock out a user when they breach a rule, limit damage and, with stored system logs, can help organizations easily meet required regulations."). On information and belief, OpenText eDOCS determines whether a document contains sensitive information in order to determine which

documents to protect against certain behaviors.

72. Open Text performs the step of "*responsive to the target document containing the sensitive information, the agent determining whether the current process activity is to be blocked allowed or modified.*" For example, if the target document contains sensitive information, the OpenText eDOCS agent determines whether the current process activity is to be blocked, allowed, or modified.

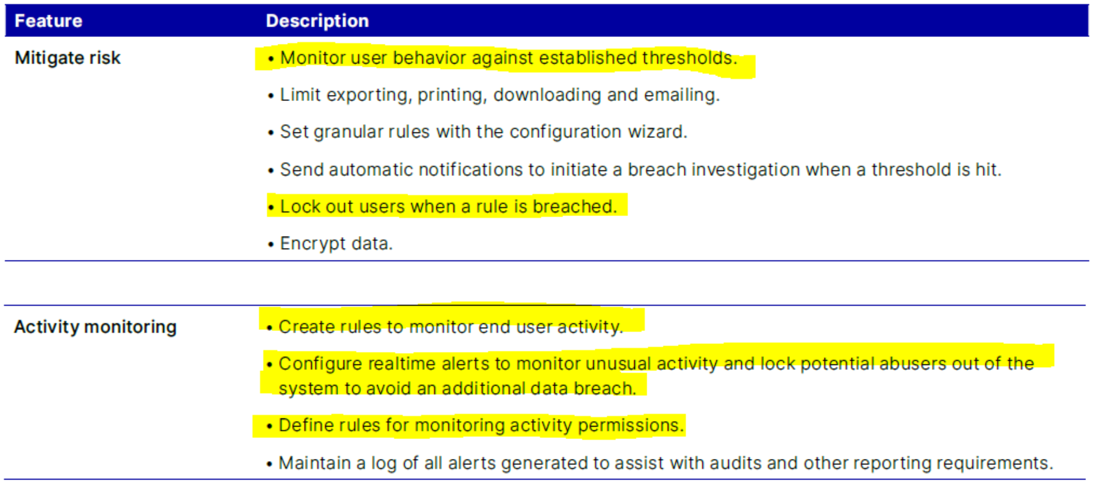


Feature	Description
Mitigate risk	• Monitor user behavior against established thresholds. • Limit exporting, printing, downloading and emailing. • Set granular rules with the configuration wizard. • Send automatic notifications to initiate a breach investigation when a threshold is hit. • Lock out users when a rule is breached. • Encrypt data.
Activity monitoring	• Create rules to monitor end user activity. • Configure realtime alerts to monitor unusual activity and lock potential abusers out of the system to avoid an additional data breach. • Define rules for monitoring activity permissions. • Maintain a log of all alerts generated to assist with audits and other reporting requirements.

See OpenText eDOCS Defense Data Sheet at 2.

73. Open Text performs the step of "*wherein after the agent identifies the target document and the associated current process activity, the agent holds the current process activity, notifies a behavior analysis engine of the target document and the current process activity, and waits for a signal from the behavior analysis engine indicating whether to continue with the current process activity.*" For example, as illustrated below, OpenText eDOCS Defense monitors user behavior against established thresholds, which on information and belief, is performed by a behavior analysis engine. The behavior analysis engine determines whether to continue with the current process activity depending on whether the user's behavior exceeds an established threshold. Thus, on information and belief, OpenText eDOCs agent identifies the target document and the associated current process activity, holds the current process activity,

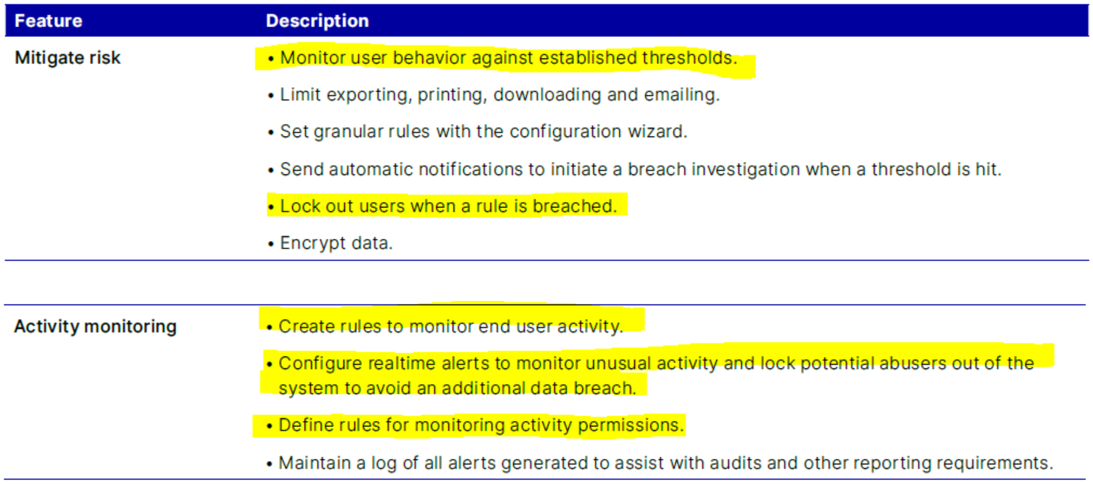
notifies a behavior analysis engine of the target document and the current process activity, and waits for a signal from the behavior analysis engine indicating whether to continue with the current process activity.



Feature	Description
Mitigate risk	• Monitor user behavior against established thresholds. • Limit exporting, printing, downloading and emailing. • Set granular rules with the configuration wizard. • Send automatic notifications to initiate a breach investigation when a threshold is hit. • Lock out users when a rule is breached. • Encrypt data.
Activity monitoring	• Create rules to monitor end user activity. • Configure realtime alerts to monitor unusual activity and lock potential abusers out of the system to avoid an additional data breach. • Define rules for monitoring activity permissions. • Maintain a log of all alerts generated to assist with audits and other reporting requirements.

See OpenText eDOCS Defense Data Sheet at 2.

74. Open Text performs the step of "*wherein the agent raises an exception and stops the current process activity if the agent is signaled by the behavior analysis engine to block the current process activity, otherwise the agent lets the current process activity to continue*." For example, as illustrated below, OpenText eDOCS Defense monitors user behavior against established thresholds, which on information and belief, is performed by a behavior analysis engine. The behavior analysis engine creates rules to monitor end user activity, configure real time alerts to monitor unusual activity and lock potential abusers out of the system. Thus, on information and belief, the OpenText eDOCS agent raises an exception and stops the current process activity if the agent is signaled by the behavior analysis engine to block the current process activity, and otherwise, the agent lets the current process activity to continue.



Feature	Description
Mitigate risk	• Monitor user behavior against established thresholds. • Limit exporting, printing, downloading and emailing. • Set granular rules with the configuration wizard. • Send automatic notifications to initiate a breach investigation when a threshold is hit. • Lock out users when a rule is breached. • Encrypt data.
Activity monitoring	• Create rules to monitor end user activity. • Configure realtime alerts to monitor unusual activity and lock potential abusers out of the system to avoid an additional data breach. • Define rules for monitoring activity permissions. • Maintain a log of all alerts generated to assist with audits and other reporting requirements.

See OpenText eDOCS Defense Data Sheet at 2.

75. Open Text has had actual knowledge of the ’487 patent since at least the filing of Trend Micro’s Counterclaims on May 16, 2022.

76. To the extent the marking requirement applies with respect to the ’487 patent, Trend Micro has a practice of marking at least its product manuals with the patents that the product practices.

77. Open Text and its partners, customers, and end users of its ’487 Accused Products and corresponding systems and services, directly infringe at least claim 1 of the ‘487 patent, literally or under the doctrine of equivalents, at least by using the ’487 Accused Products as described above. On information and belief, the infringing actions of Open Text’s partners, customers, and end users of the ’487 Accused Products are attributable to Open Text. For example, Open Text direct and control their partners by contractual agreement to operate, or to provide Open Text with the means to operate (*e.g.*, servers), or otherwise distribute the ’487 Accused Products in a manner that infringes the ’487 patent. Open Text further conditions receipt of benefit of the ’487 Accused Products upon use of the patented features, such as performing steps of the methods claimed in the ’487 patent.

78. In addition to Counter-Defendant Open Text's and its customers' direct infringement, Open Text has infringed and continues to infringe the '487 patent indirectly, including by actively inducing others to directly infringe at least claim 1 of the '487 patent in violation of 35 U.S.C. § 271(b).

79. For example, Open Text encourages and induces customers to use the '487 Accused Products in a manner that infringes claim 1 of the '487 patent by at least offering and providing software that performs a method that infringes claim 1 when installed and operated by the customers, and by activities related to selling, marketing, advertising, promotion, installation, support, and distribution of the '487 Accused Products.

80. Open Text encourages and induces third parties to use the '487 Accused Products in a manner that infringes the '487 patent as described above, including through advertising, marketing, customer support, user manuals, instructions, installation, and distribution of the '487 Accused Products in the United States. For example, Open Text's customers and end users test and/or operate OpenText eDOCS in the United States in accordance with Open Text's instructions contained in, for example, its user manuals, thereby also performing the claimed methods and infringing the asserted claims of the '487 Patent reciting such operation. *See* OpenText eDOCS Defense Data Sheet.

81. Moreover, Open Text contributes to infringement of the '487 patent by, among other activities, making, using, offering for sale, selling within the United States, and/or importing into the United States the '487 Accused Products with knowledge that such activities practice every element of one or more claims of the '487 patent, or being willfully blind to such activities practicing every element of one or more claims of the '487 patent. Open Text's affirmative acts of making, offering for sale, selling, and/or importing into the United States the

’487 Accused Products contribute to Open Text’s customers and end-users infringing of the ’487 Accused Products. The infringing software components of the ’487 Accused Products are specially designed in a way that infringes one or more claims of the ’487 patent and can be used only in a manner that infringes the ’487 patent and thus have no substantial non-infringing uses.

82. The above description regarding Open Text’s infringement of the ’487 patent is based on publicly available information and a reasonable investigation of the operation of the ’487 Accused Products. Trend Micro reserves the right to modify this description, including, for example, on the basis of information about the ’487 Accused Products that it obtains during discovery.

83. Unless and until enjoined by this Court, Open Text will continue to infringe the ’487 patent. Open Text’s infringement is causing and will continue to cause Trend Micro irreparable harm, for which there is no remedy at law.

84. Under 35 U.S.C. § 283, Trend Micro is entitled to a preliminary and permanent injunction against further infringement of the ’487 patent.

85. Open Text’s infringement of the ’487 patent has been knowing and willful since at least the filing of Trend Micro’s Counterclaims on May 16, 2022.

86. Trend Micro has suffered and continues to suffer damages, including lost profits, as a result of Open Text’s infringement of the ‘487 patent. Under 35 U.S.C. § 284, Trend Micro is entitled to damages adequate to compensate it for Open Text’s infringement, in no event less than a reasonable royalty for Open Text’s use of the inventions of the ’487 patent, together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Trend Micro seeks the following relief:

That Webroot and Open Text have directly infringed the Trend Micro Patents-in-Suit under 35 U.S.C. § 271(a);

That Webroot and Open Text are inducing infringement of the Trend Micro Patents-in-Suit under 35 U.S.C. § 271(b);

That Webroot and Open Text are contributory infringers of the Trend Micro Patents-in-Suit under 35 U.S.C. § 271(c);

That Webroot, Open Text, and any of its affiliates, subsidiaries, officers, directors, employees, agents, representatives, licensees, successors, assigns, and all those acting for any of them and/or any of their behalf, or acting in concert with any of them directly or indirectly, be preliminarily and permanently enjoined from infringing, inducing others to infringe, or contributing to others' infringement of the Trend Micro Patents-in-Suit.

That Webroot and Open Text be ordered to pay compensatory damages to Trend Micro, together with pre-judgment interest post-judgment interest, and costs as allowed by law;

That Webroot and Open Text be ordered to provide an accounting, including a post-verdict and post-judgment accounting for any infringement not otherwise covered by a damages award or the requested injunctive relief;

That Webroot and Open Text be ordered to pay supplemental damages to Trend Micro, including without limitation, interest;

That the infringement by Webroot and Open Text be adjudged willful and that the damages be increased under 35 U.S.C. § 284 to three times the amount found or measured;

That the Court determine this is an exceptional case under 35 U.S.C. § 285 and an award of attorneys' fees and costs to Trend Micro is warranted in this action; and

For any such other and further relief as the Court deems just and equitable.

JURY DEMAND

In accordance with Rule 38 of the Federal Rules of Civil procedure, Trend Micro hereby demands trial by jury on all issues triable to a jury in this action.

DATED: May 16, 2022

PAUL HASTINGS LLP

By: */s/ Yar R. Chaikovsky*
Yar R. Chaikovsky, Bar No. 39625
yarchaikovsky@paulhastings.com
Philip Ou
philipou@paulhastings.com
Bruce Yen
bruceyen@paulhastings.com
Radhesh Devendran
radheshdevendran@paulhastings.com

1117 S. California Avenue
Palo Alto, California 94304-1106
Telephone: 1(650) 320-1800
Facsimile: 1(650) 320-1900

Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that on May 16, 2022, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system which will send notification of such filing via electronic mail to all counsel of record.

/s/ Yar R. Chaikovsky
Yar R. Chaikovsky